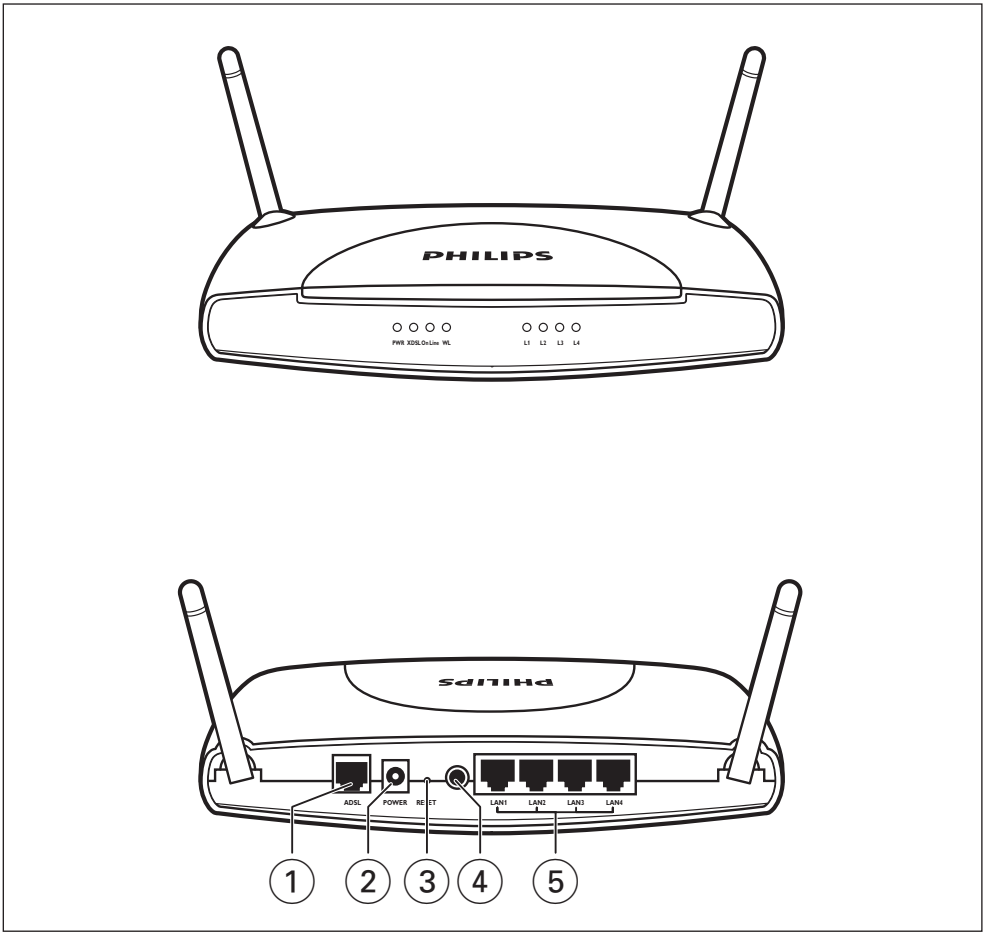
CPWBS154

Instructions for use

PHILIPS



1 **ADSL Port**
WAN port (RJ-11). Connect your ADSL line to this port.

2 **Power Inlet**
Connect the included power adapter to this inlet.
Warning: *Using the wrong type of power adapter may damage the ADSL Wireless Base Station.*

3 **Reset Button**
Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see 'Reset' on page 54-55.

4 **Power button**
Press this button to turn on/turn off the ADSL Wireless Base Station.

5 **LAN Ports**
10/100 Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch).

Table of Contents

Introduction

CPWBS154

Congratulations on your purchase of the Philips ADSL Wireless Base Station, hereafter referred to as the 'ADSL Wireless Base Station'. We are proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet.
For those who want to surf the Internet in the most secure way, this router provides a convenient and powerful solution.

About the ADSL Wireless Base Station

The ADSL Wireless Base Station provides Internet access to multiple users by sharing a single-user account. Support is provided for both wired and wireless devices. New technology provides wireless security via Wired Equivalent Privacy (WEP) encryption and MAC address filtering. It is simple to configure and can be up and running in minutes.

Features and Benefits

- Internet connection to an ADSL line via an RJ-11 ADSL port
- Local network connection via four 10/100 Mbps Ethernet ports
- On-board IEEE 802.11g wireless network adapter
- DHCP for dynamic IP configuration, and DNS for domain name mapping
- Firewall with Stateful Packet Inspection, client privileges, intrusion detection, and NAT
- NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet services such as web, FTP, email, and Telnet)
- VPN pass-through (IPSec-ESP Tunnel mode, L2TP, PPTP)
- User-definable application sensing tunnel supports applications requiring multiple connections
- Easy setup through a web browser on any operating system that supports TCP/IP
- Compatible with all popular Internet applications

Applications

Many advanced networking features are provided by the ADSL Wireless Base Station:

Wireless and Wired LAN

The ADSL Wireless Base Station provides connectivity to 10/100 Mbps devices, and wireless IEEE 802.11g compatible devices, making it easy to create a network in small offices or homes.

Internet Access

This device supports Internet access through an ADSL connection. Since many DSL providers use PPPoE or PPPoA to establish communications with end users, the ADSL Wireless Base Station includes built-in clients for these protocols, eliminating the need to install these services on your computer.

Shared IP Address
The ADSL Wireless Base Station provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can browse the web at the same time.

Virtual Server
If you have a fixed IP address, you can set the ADSL Wireless Base Station to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the ADSL Wireless Base Station can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

DMZ Host Support
Allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly.

Security
The ADSL Wireless Base Station supports security features that deny Internet access to specified users, or filter all requests for specific services that the administrator does not want to serve. The ADSL Wireless Base Station's firewall also blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. WEP (Wired Equivalent Privacy), SSID, and MAC filtering provide security over the wireless network.

Important information

- Please install and connect the product in the order as described in the chapter 'Before You Start Guide' only. This assures best installation results with the least technical hassles.
- Please read this guide carefully before using the ADSL Wireless Base Station; and keep it for future reference.
- During set-up and installation, it may be helpful to have the instructions for your PC and other network components at hand.

Safety Precautions

- Do not expose the product to excessive moisture, rain, sand or heat sources.
- The product should not be exposed to dripping or splashing. No object filled with liquids, such as vases, should be placed on the product.
- Keep the product away from domestic heating equipment and direct sunlight.
- Allow a sufficient amount of free space all around the product for adequate ventilation.
- Do not open this product. Contact your retailer if you experience technical difficulties.

Environmental information

All redundant packing material has been omitted. We have done our utmost to make the packaging easily separable into three mono materials: cardboard (box), polystyrene foam (buffer) and polyethylene (bags, protective foam sheet). Your set consists of materials that can be recycled if disassembled by a specialised company. Please observe the local regulations regarding the disposal of packing materials, exhausted batteries and old equipment.

Packaging contents

Please check whether all of the following items are present in the box of the Wireless Base Station. These are provided to help you set up and use your Wireless Base Station. Contact your retailer if any items are missing.

- Philips ADSL Wireless Base Station
- Power adapter
- One Category 5 Ethernet cable (RJ-45)
- Telephone patch cable (RJ-11)
- 'Before You Start' Card
- CD with manual

Disclaimer

This product is provided by 'Philips' 'as is" and without any express or implied warranty of any kind of warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed.

In no event shall Philips be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of information, data, or profits; or business interruption) howsoever caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of inability to use this product, even if advised of the possibility of such damages.

Philips further does not warrant the accuracy or completeness of the information, text, graphics, illustrative examples links or other items can be deviated of the product.

Installation

System Requirements

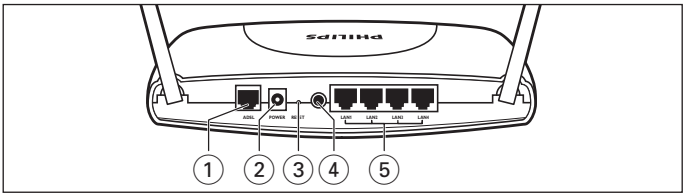
- ADSL line installed by your Internet Service Provider.
- A computer using a fixed IP address or dynamic IP address assigned via DHCP, as well as a gateway server address and DNS server address from your service provider.
- A computer equipped with a 10/100 Mbps network adapter, a USB-to-Ethernet converter or an IEEE 802.11g wireless network adapter.
- TCP/IP network protocols installed on each PC that will access the Internet.
- A Java-enabled web browser, such as Microsoft Internet Explorer 5.5 or above or Netscape 4.7 or above, installed on one PC at your site for configuring the ADSL Wireless Base Station.

Hardware Description

The ADSL Wireless Base Station contains an integrated ADSL modem and connects to the Internet or to a remote site using its RJ-11 WAN port. It can be connected directly to your PC or to a local area network using any of the four 10/100 Ethernet LAN ports.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the 10/100 Ethernet ports and 54 Mbps over the built-in wireless network adapter.

The ADSL Wireless Base Station includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting. It also provides the following ports on the rear panel:



1 ADSL Port
WAN port (RJ-11). Connect your ADSL line to this port.

2 Power Inlet
Connect the included power adapter to this inlet.
Warning: *Using the wrong type of power adapter may damage the ADSL Wireless Base Station.*

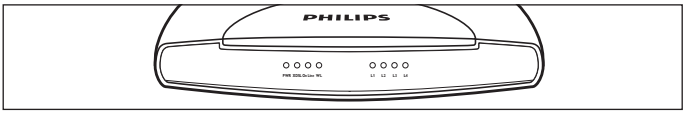
3 Reset Button
Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see 'Reset' on page 54-55.

4 Power button
Press this button to turn on/turn off the ADSL Wireless Base Station.

5 LAN Ports
10/100 Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch).

LED Indicators

The power and port LED indicators on the front panel are illustrated by the following figure and table.



LED	Status	Description
PWR (Power)	On	Power on, normal operation.
	Off	Power off or failure.
xDSL (DSL sync)	On	ADSL loop is brought UP.
	Blinking	Start up.
	Off	ADSL loop is down.
Online	On	Link is up.
	Blinking	Send/Receive data.
	Off	No data transfering.
WL (Wireless)	On	Link is up.
	Blinking	Send/Receive data.
	Off	No data transfering.
LAN 1-4	On	Ethernet Connection is established.
	Blinking	Send/Receive data.
	Off	Without Link.

ISP Settings

Please collect the following information from your ISP before setting up the ADSL Wireless Base Station:

- ISP account user name and password
- Protocol, encapsulation and VPI/VCI circuit numbers
- DNS server address
- IP address, subnet mask and default gateway (for fixed IP users only)

Connect the System

The ADSL Wireless Base Station can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines:

- Keep the ADSL Wireless Base Station away from any heating devices.
- Do not place the ADSL Wireless Base Station in a dusty or wet environment.

You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the ADSL Wireless Base Station.

Connect the ADSL Line

Connect the supplied RJ-11 cable from the ADSL Microfilter/Splitter to the ADSL port on your ADSL Wireless Base Station. When inserting an ADSL RJ-11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Phone Line Configuration

Installing a Full-Rate Connection

If you are using a full-rate (G.dmt) connection, your service provider will attach the outside ADSL line to a data/voice splitter. In this case you can connect your phones and computer directly to the splitter as shown below:

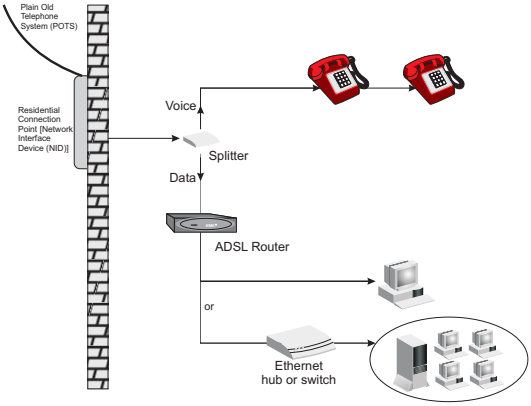


Figure 2-3. Installing with a Splitter

Installing a Splitterless Connection

If you are using a splitterless (G.lite) connection, then your service provider will attach the outside ADSL line directly to your phone system.
In this case you can connect your phones and computer directly to the incoming ADSL line, but you will have to add low-pass filters to your phones as shown below:

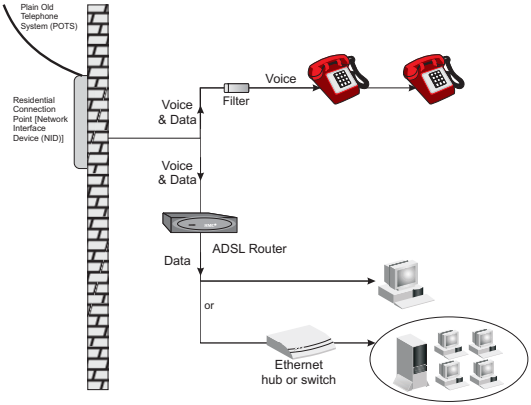


Figure 2-4. Installing without a Splitter

Attach to Your Network Using Ethernet Cabling
The four LAN ports on the ADSL Wireless Base Station auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half duplex or full duplex.

Use RJ-45 cables to connect any of the four LAN ports on the ADSL Wireless Base Station to an Ethernet adapter on your PC. Otherwise, cascade any of the LAN ports on the ADSL Wireless Base Station to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that it is properly seated.

Warning: *Do not plug a phone jack connector into an RJ-45 port. This may damage the ADSL Wireless Base Station.*

Notes:
– *Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all 10/100 ethernet ports. Use Category 3, 4, or 5 for connections that operate at 10 Mbps, and Category 5 for connections that operate at 100 Mbps.*
– *Make sure each twisted-pair cable length does not exceed 100 meters (328 feet).*

Connect the Power Adapter
Plug the power adapter into the power socket on the rear of the ADSL Wireless Base Station, and the other end into a power outlet.

Check the power indicator on the front panel is lit. If the power indicator is not lit, refer to 'Troubleshooting' on page 67-68.

In case of a power input failure, the ADSL Wireless Base Station will automatically restart and begin to operate once the input power is restored.

Configuring Client PC

After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the ADSL Wireless Base Station.

See: 'Windows 98/Me' on page 11-13
'Windows NT 4.0' on page 15-17
'Windows 2000' on page 19
'Windows XP' on page 21
or 'Configuring Your Macintosh Computer' on page 22-23
depending on your operating system.

TCP/IP Configuration

To access the Internet through the ADSL Wireless Base Station, you must configure the network settings of the computers on your LAN to use the same IP subnet as the ADSL Wireless Base Station. The default IP settings for the ADSL Wireless Base Station are:

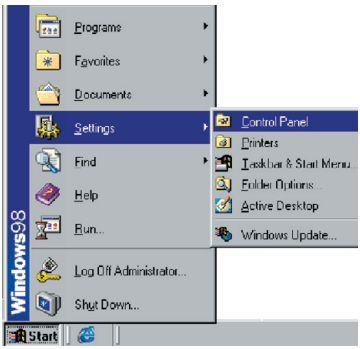
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP function	Enable
DHCP IP Pool Range	192.168.1.2 to 192.168.1.254

Note: *These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the ADSL Wireless Base Station's web configuration interface in order to make the required changes. (See 'Configuring the ADSL Wireless Base Station' on page 25 for instruction on configuring the ADSL Wireless Base Station.)*

Windows 98/Me

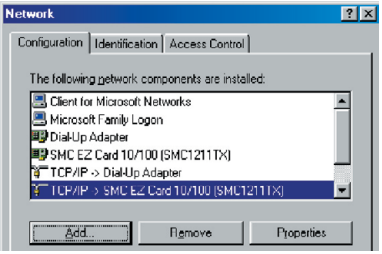
You may find that the instructions in this section do not exactly match your version of Windows. This is because these steps and screen shots were created from Windows 98. Windows Millennium Edition is similar, but not identical, to Windows 98.

1 On the Windows desktop, click Start/Settings/Control Panel.

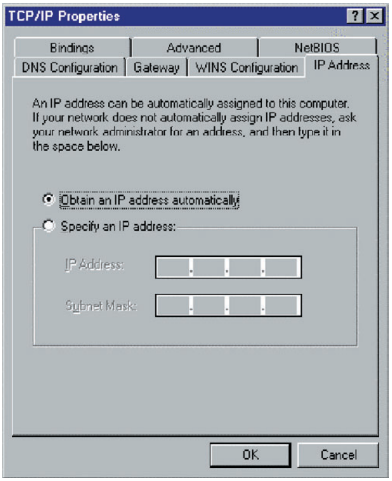


2 In Control Panel, double-click the Network icon.

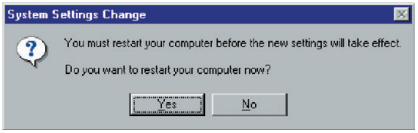
3 In the Network window, under the Configuration tab, double-click the TCP/IP item listed for your network card.



4 In the TCP/IP window, select the IP Address tab. If 'Obtain an IP address automatically' is already selected, your computer is already configured for DHCP. If not, select this option.



5 Windows may need your Windows 98/Me CD to copy some files. After it finishes copying, it will prompt you to restart your system. Click Yes and your computer will restart.



TCP/IP Configuration Setting

Primary DNS Server _____.____.____.____
Secondary DNS Server _____.____.____.____
Default Gateway _____.____.____.____
Host Name _____.____.____.____

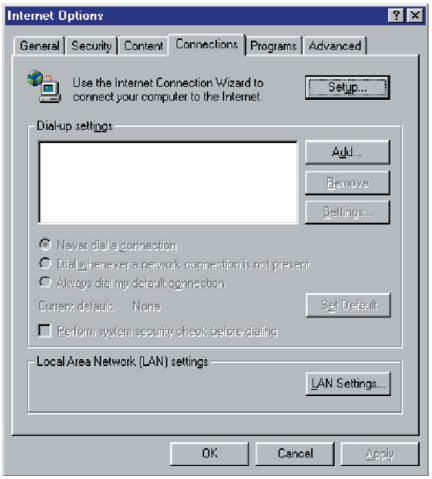
Disable HTTP Proxy

You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the ADSL Wireless Base Station's HTML configuration pages. The following steps are for Internet Explorer.

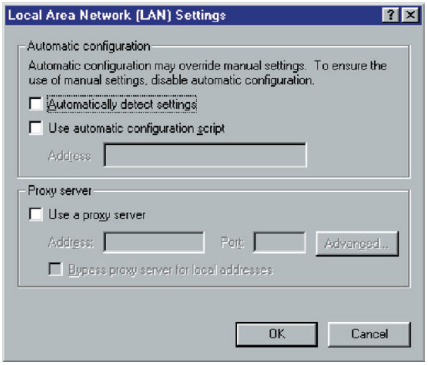
Internet Explorer

1 Open Internet Explorer.
2 Click the Stop button, then click Tools/Internet Options.

3 In the Internet Options window, click the Connections tab. Next, click the LAN Settings... button.



4 Clear all the check boxes.
5 Click OK, and then click OK again to close the Internet Options window.

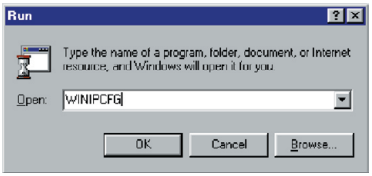


Obtain IP Settings from Your ADSL Wireless Base Station

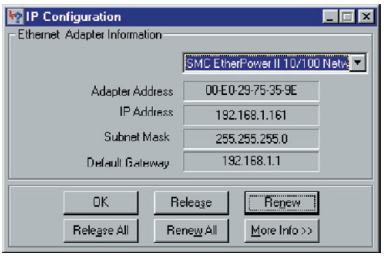
Now that you have configured your computer to connect to your ADSL Wireless Base Station, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your ADSL Wireless Base Station, you can also verify that you have configured your computer correctly.

1 On the Windows desktop, click Start/Run...

2 Type 'WINIPCFG' and click OK.
It may take a second or two for the IP Configuration window to appear.

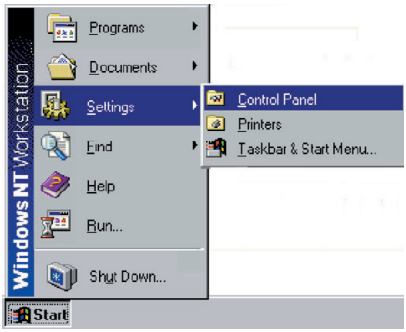


3 In the IP Configuration window, select your network card from the drop-down menu. Click Release and then click Renew. Verify that your IP address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.1. These values confirm that your ADSL Wireless Base Station is functioning. Click OK to close the IP Configuration window.

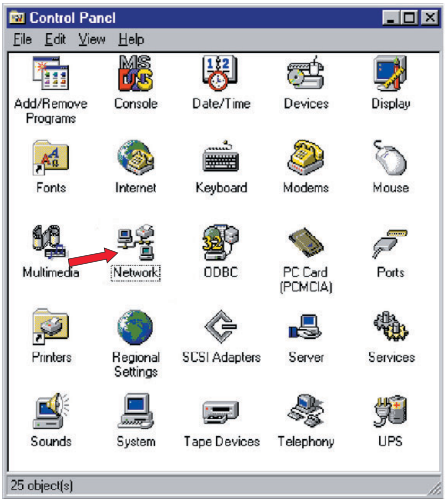


Windows NT 4.0

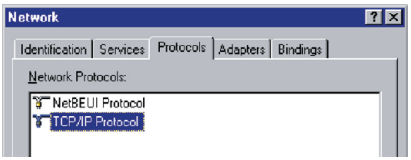
1 On the Windows desktop, click Start/Settings/Control Panel.



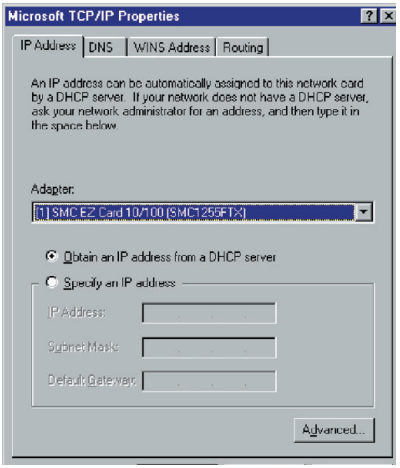
2 Double-click the Network icon.



3 In the Network window, select the Protocols tab. Double-click TCP/IP Protocol.



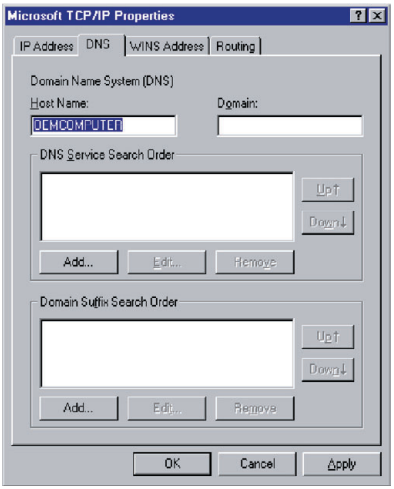
4 When the Microsoft TCP/IP Properties window opens, select the IP Address tab.



5 In the Adapter drop-down list, make sure your Ethernet adapter is selected.

6 If 'Obtain an IP address automatically' is already selected, your computer is already configured for DHCP. If not, select this option and click 'Apply.'

7 Click the DNS tab to see the primary and secondary DNS servers. Record these values, and then click 'Remove.' Click 'Apply', and then 'OK.'



8 Windows may copy some files, and will then prompt you to restart your system. Click Yes and your computer will shut down and restart.

TCP/IP Configuration Setting

Primary DNS Server	____.____.____.____
Secondary DNS Server	____.____.____.____
Default Gateway	____.____.____.____
Host Name	____.____.____.____

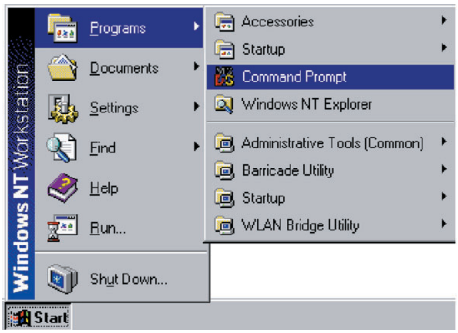
Disable HTTP Proxy

You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the ADSL Wireless Base Station's HTML configuration pages (refer to 'Internet Explorer' on page 13).

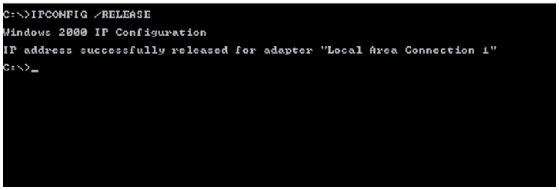
Obtain IP Settings from Your ADSL Wireless Base Station

Now that you have configured your computer to connect to your ADSL Wireless Base Station, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your ADSL Wireless Base Station, you will verify that you have configured your computer correctly.

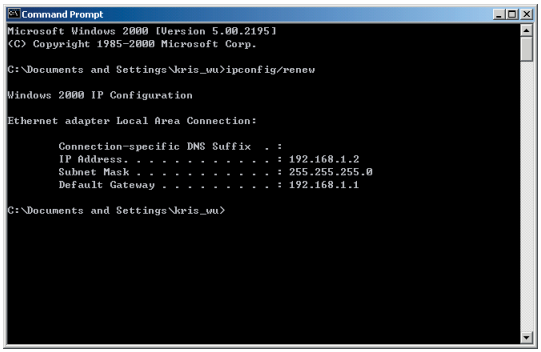
1 On the Windows desktop, click Start/Programs/Command Prompt.



2 In the Command Prompt window, type 'IPCONFIG /RELEASE' and press the ENTER key.



3 Type 'IPCONFIG /RENEW' and press the ENTER key. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.1.
These values confirm that your ADSL Wireless Base Station is functioning.



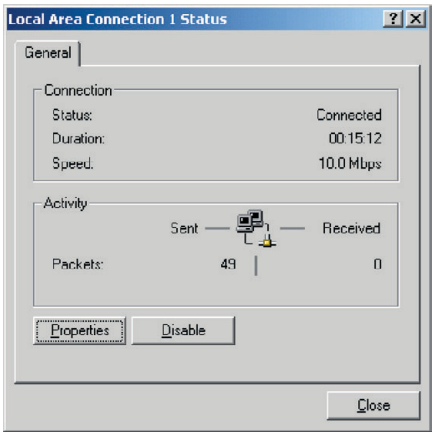
4 Type 'EXIT' and press the ENTER key to close the Command Prompt window.
Your computer is now configured to connect to the ADSL Wireless Base Station.

Windows 2000

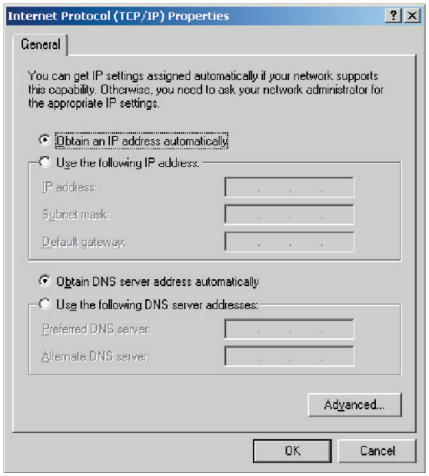
1 On the Windows desktop, click Start/Settings/Network and Dial-Up Connections.

2 Click the icon that corresponds to the connection to your ADSL Wireless Base Station.

3 The connection status screen will open. Click Properties.



4 Double-click Internet Protocol (TCP/IP).



5 If 'Obtain an IP address automatically' and 'Obtain DNS server address automatically' are already selected, your computer is already configured for DHCP. If not, select this option.

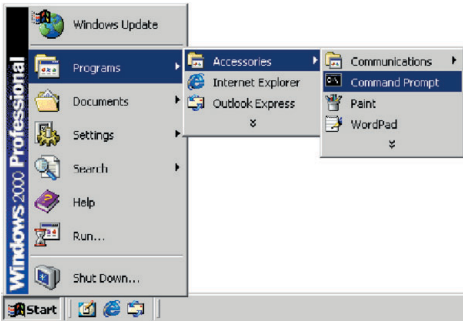
Disable HTTP Proxy

You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the ADSL Wireless Base Station's HTML configuration pages (refer to 'Internet Explorer' on page 13).

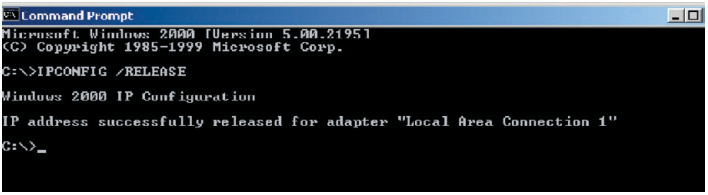
Obtain IP Settings from Your ADSL Wireless Base Station

Now that you have configured your computer to connect to your ADSL Wireless Base Station, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your ADSL Wireless Base Station, you can verify that you have configured your computer correctly.

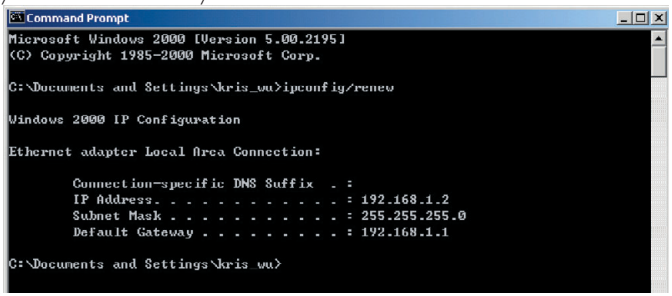
1 On the Windows desktop, click Start/Programs/Accessories/Command Prompt.



2 In the Command Prompt window, type 'IPCONFIG/RELEASE' and press the ENTER key.



3 Type 'IPCONFIG /RENEW' and press the ENTER key. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.1.



These values confirm that your ADSL Wireless Base Station is functioning.

4 Type 'EXIT' and press the ENTER key to close the Command Prompt window.

Your computer is now configured to connect to the ADSL Wireless Base Station.

Windows XP

1 On the Windows desktop, click Start/Control Panel.

2 In the Control Panel window, click Network and Internet Connections.

3 The Network Connections window will open.
Double-click the connection for this device.

4 On the connection status screen, click Properties.

5 Double-click Internet Protocol (TCP/IP).

6 If 'Obtain an IP address automatically' and 'Obtain DNS server address automatically' are already selected, your computer is already configured for DHCP. If not, select this option.

Disable HTTP Proxy
You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the ADSL Wireless Base Station's HTML configuration pages (refer to 'Internet Explorer' on page 13).

Obtain IP Settings from Your ADSL Wireless Base Station
Now that you have configured your computer to connect to your ADSL Wireless Base Station, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your ADSL Wireless Base Station, you can verify that you have configured your computer correctly.

1 On the Windows desktop, click Start/Programs/Accessories/Command Prompt.

2 In the Command Prompt window, type 'IPCONFIG/RELEASE' and press the ENTER key.

3 Type 'IPCONFIG /RENEW' and press the ENTER key. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.1. These values confirm that your ADSL Wireless Base Station is functioning.
Type 'EXIT' and press the ENTER key to close the Command Prompt window.

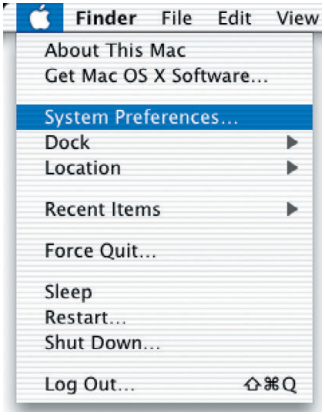
Your computer is now configured to connect to the ADSL Wireless Base Station.

Configuring Your Macintosh Computer

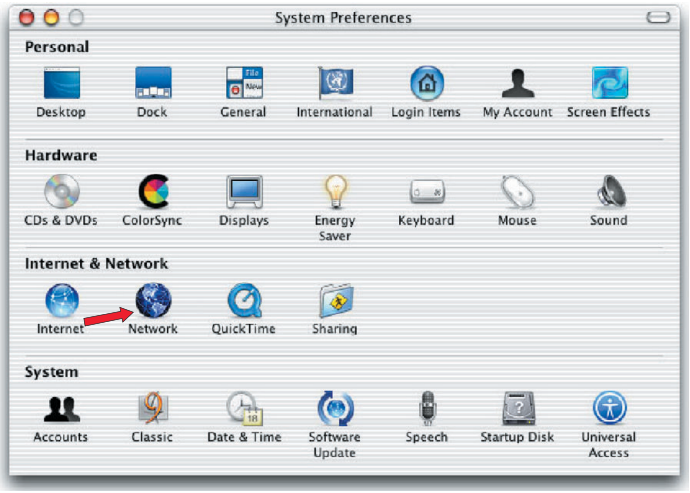
You may find that the instructions here do not exactly match your operating system. This is because these steps and screen shots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:

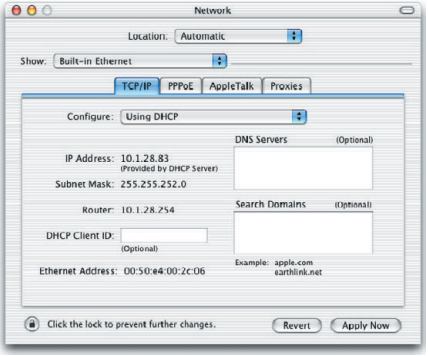
1 Pull down the Apple Menu. Click System Preferences.



2 Double-click the Network icon in the Systems Preferences window.



3 If 'Using DHCP Server' is already selected in the Configure field, your computer is already configured for DHCP. If not, select this Option.



4 Your new settings are shown on the TCP/IP tab. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.1. These values confirm that your ADSL Wireless Base Station is functioning.

5 Close the Network window.

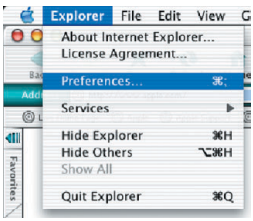
Now your computer is configured to connect to the ADSL Wireless Base Station.

Disable HTTP Proxy

You need to verify that the 'HTTP Proxy' feature of your web browser is disabled. This is so that your browser can view the ADSL Wireless Base Station's HTML configuration pages. The following steps are for Internet Explorer.

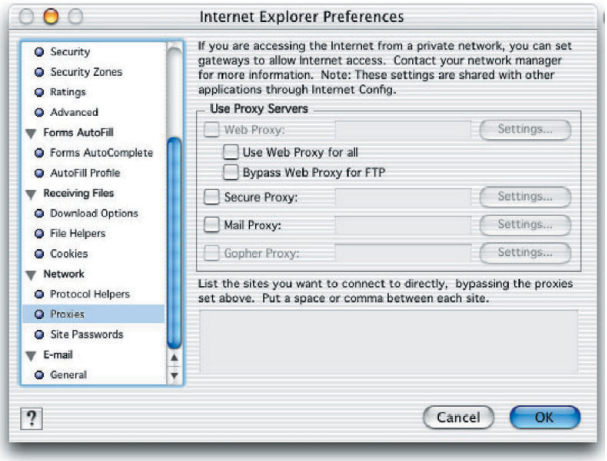
Internet Explorer

1 Open Internet Explorer and click the Stop button.
Click Explorer/Preferences.



2 In the Internet Explorer Preferences window, under Network, select Proxies.

3 Uncheck all check boxes and click OK.



Configuring the ADSL Wireless Base Station

Setup Wizard

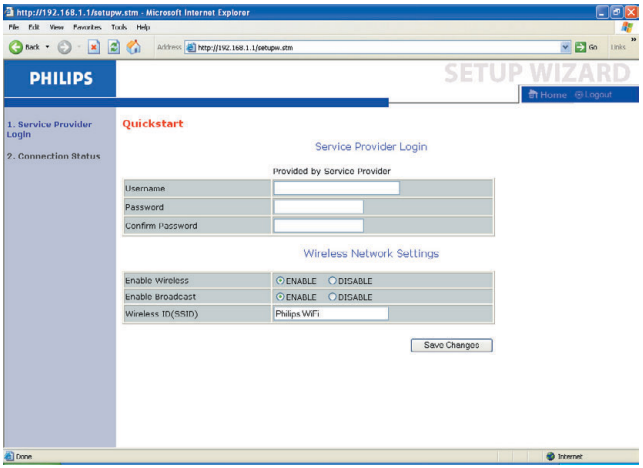
Quickstart

Service Provider Login

This part allows you to enter the Username and Password as provided by your Internet Service Provider.

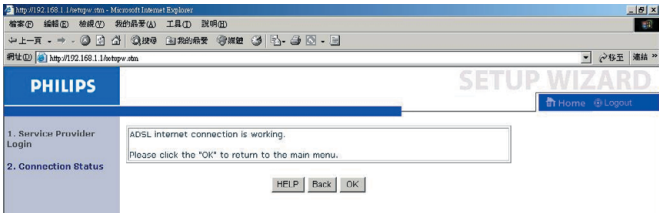
Wireless Network Settings

Here you can enable or disable the wireless networking functionality of this Router. When Wireless is enabled, broadcasting your Wireless ID can be enabled or disabled. The Wireless ID (SSID) is the name you wish your network to have.



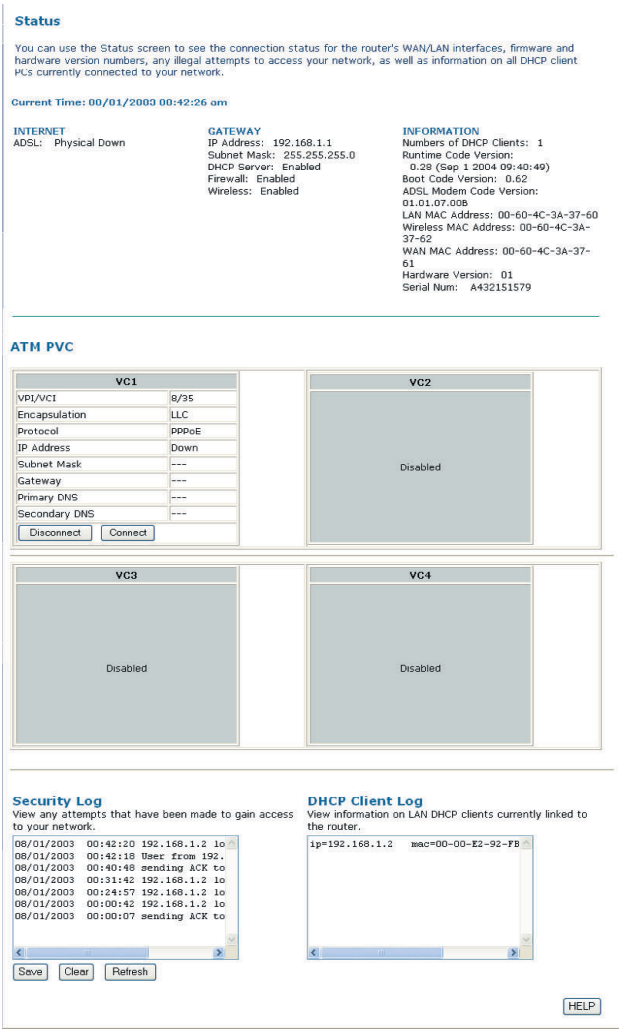
After entering these settings, click 'Save Changes' to confirm.

When you entered the correct Username and Password, and confirmed these settings, the following screen will appear, telling you the ADSL connection is now operational.



Confirm

The Confirm page shows a summary of the configuration parameters.



ADSL

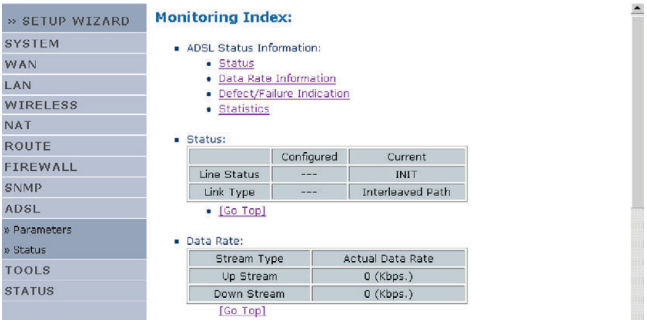
ADSL (Asymmetric Digital Subscriber Line) is designed to deliver more bandwidth downstream (from the central office to the customer site) than upstream. This section is used to configure the ADSL operation type and shows the ADSL status.

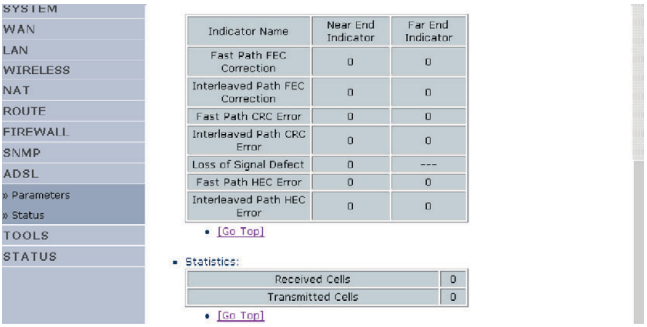
Parameter	Description
Operation Mode	• Automatic • T1.413 issue 2 • G.992.1 • G.992.2

This page is designed for the engineer to test the ADSL loop condition. Therefore, it is advised that users should not change the settings here at all.

Status

The Status screen displays information on connection line status, data rate, operation data and defect indication, and statistics.



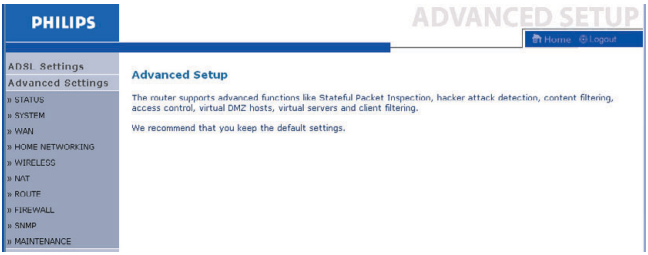


The following items are included on the ADSL status page:

Parameter	Description
Status	
• Line Status	Shows the current status of the ADSL line connection.
• Link Type	Two types of link: Fast path and Interleaved path.
Data Rate	
• Upstream	Maximum upstream data rate.
• Downstream	Maximum downstream data rate.
Operation Data/ Defect Indication	
• Noise Margin	Maximum upstream and downstream noise margin.
• Attenuation	Maximum reduction in the strength of the upstream and downstream signal.
• Fast Path FEC Correction	There are two latency paths that may be used: fast and interleaved. For either path, a forward error correction (FEC) scheme is employed to ensure higher data integrity. For maximum noise immunity, an interleaver may be used to supplement FEC.
• Interleaved Path FEC Correction	An interleaver is basically a buffer used to introduce a delay, allowing for additional error correction techniques to handle noise. Interleaving slows the data flow and may not be optimal for real-time signals such as video transmission.
Fast Path CRC Error	The number of Fast Path Cyclic Redundancy Check errors.
Interleaved Path CRC Error	The number of Interleaved Path Cyclic Redundancy Check errors.
Loss of Signal Defect	Momentary signal discontinuities.
Fast Path HEC Error	Fast Path Header Error Concealment errors.
Interleaved Path HEC Error	Interleaved Path Header Error Concealment errors.
Statistics	(Superframes represent the highest level of data presentation. Each superframe contains regular ADSL frames, one of which is used to provide superframe synchronization, identifying the start of a superframe. Some of the remaining frames are also used for special functions.)
• Received cells	Number of cells received.
• Transmitted cells	Number of cells transmitted.

Advanced Setup

Click on 'Advanced Settings' which is located on the left side of the screen. The left-hand side displays the main menu and the right-hand side shows descriptive information.

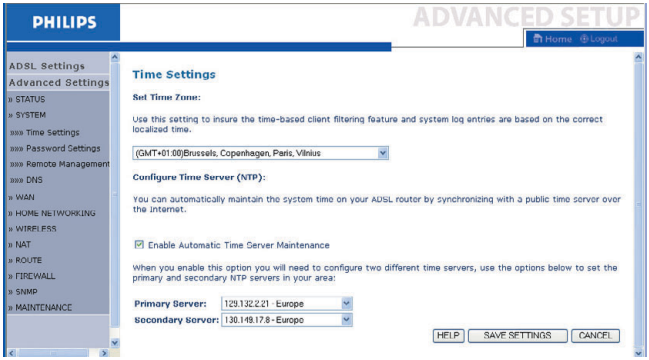


The advanced management interface contains 10 main menu items as described in the following table.

Parameter	Description
STATUS	Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and firewall information. Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number. Shows the security and DHCP client log.
SYSTEM	Sets the local time zone, the password for administrator access, and the IP address of a PC or notebook that will be allowed to manage the ADSL Wireless Base Station remotely.
WAN	Specifies the Internet connection settings.
HOME NETWORKING	Sets the TCP/IP configuration for the ADSL Wireless Base Station LAN interface and DHCP clients.
WIRELESS	Configures the radio frequency, SSID, and security for wireless communications.
NAT	Configures Address Mapping, virtual server and special applications.
ROUTE	Sets the routing parameters and displays the current routing table.
FIREWALL	Configures a variety of security and specialized functions including: Access Control, URL blocking, Internet access control scheduling, intruder detection, and DMZ.
SNMP	Community string and trap server settings.
MAINTENANCE	Contains options to backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the systems.

Time Settings

Select your local time zone from the drop down list. This information is used for log entries and client filtering.

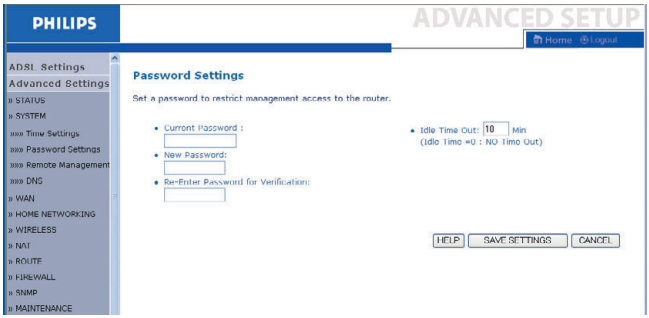


For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop down list.

If you want to automatically synchronize the ADSL Wireless Base Station with a public time server, check the box to Enable Automatic Time Server Maintenance. Select the desired servers from the drop down menu.

Password Settings

Use this page to change the password for accessing the management interface of the ADSL Wireless Base Station.



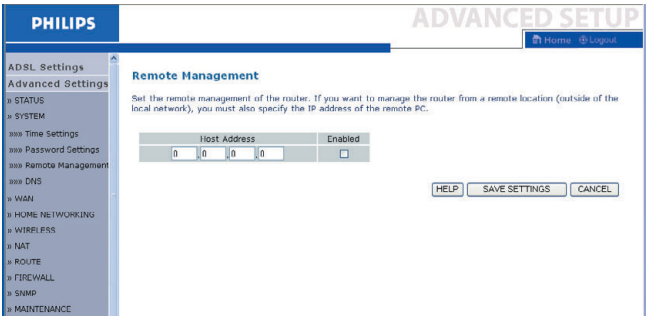
Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

Note: *If you lost the password, or you cannot gain access to the user interface, press the blue reset button on the rear panel, holding it down for at least five seconds to restore the factory defaults. By default, there is no password to login to the user interface.*

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity.
If the connection is inactive for longer than the maximum idle time, it will perform system logout, and you have to log in again to access the management interface. (Default: 10 minutes)

Remote Management

By default, management access is only available to users on your local network. However, you can also manage the ADSL Wireless Base Station from a remote host by entering the IP address of a remote computer on this screen. Check the Enabled check box, and enter the IP address of the Host Address and click 'SAVE SETTINGS'.

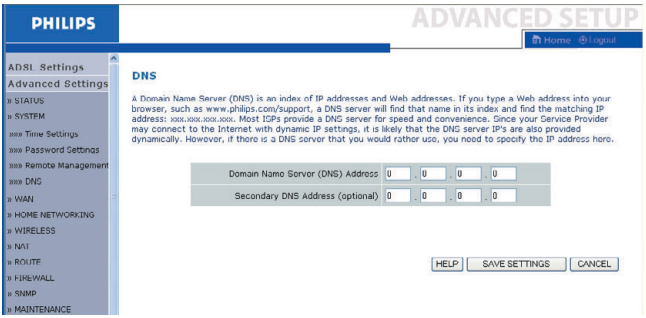


Note: *If you check Enable and specify an IP address of 0.0.0.0, any remote host can manage the ADSL Wireless Base Station.*

For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by :8080, for example, 212.120.68.20:8080.

DNS

Domain Name Servers (DNS) are used to map a domain name (e.g., www.philips.com) with the IP address (e.g., 64.147.25.20). Your ISP should provide the IP address of one or more Domain Name Servers.
Enter those addresses on this page, and click 'SAVE SETTINGS'.

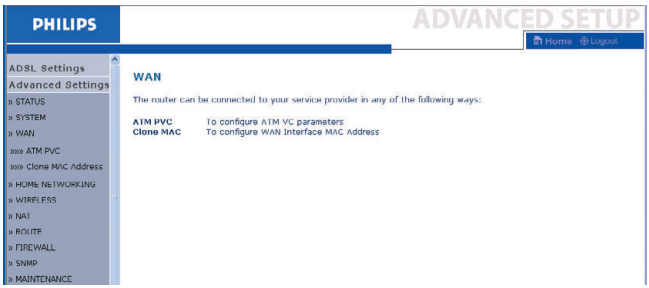


WAN

Specify the WAN connection parameters provided by your Internet Service Provider (ISP).

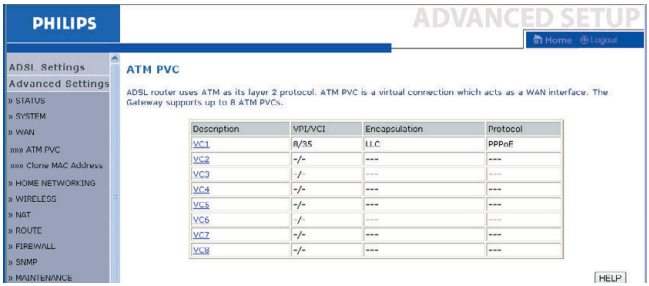
The ADSL Wireless Base Station can be connected to your ISP in one of the following ways:

- ATM PVC
- Clone MAC



ATM PVC

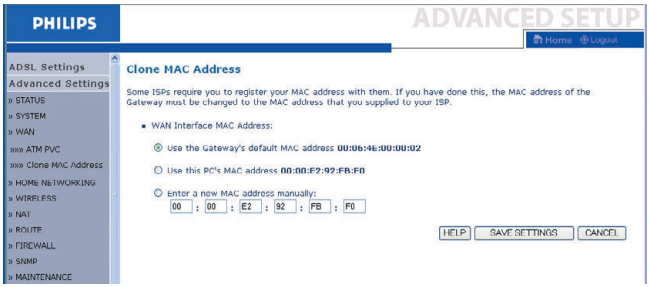
Enter the ATM (Asynchronous Transfer Mode) virtual connection parameters here.



Parameter	Description
Description	Click on the VC to set the values for the connection.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI).
Encapsulation	Specifies how to handle multiple protocols at the ATM transport layer. • VC-MUX: Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead. • LLC: Point-to-Point Protocol over ATM Logical Link Control (LLC) allows multiple protocols running over one virtual circuit (using slightly more overhead).
Protocol	Protocol used for the connection.
DHCP Client Log	Displays information on DHCP clients on your network.

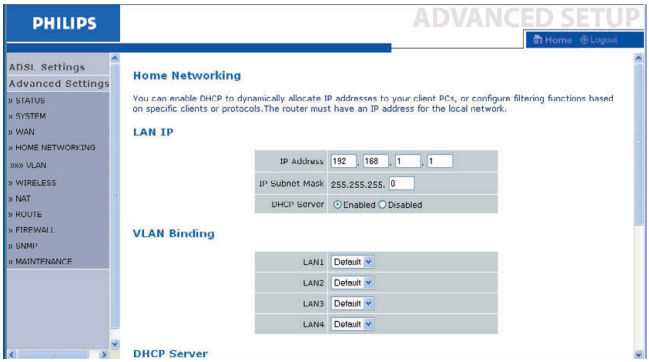
Clone MAC Address

Some ISPs require you to register your MAC address with them. If this is the case, the MAC address of the ADSL Wireless Base Station must be changed to the MAC address that you have registered with your ISP.



Home Networking

Use the Home Networking menu to configure the LAN IP address and to enable the DHCP server for dynamic client address allocation.

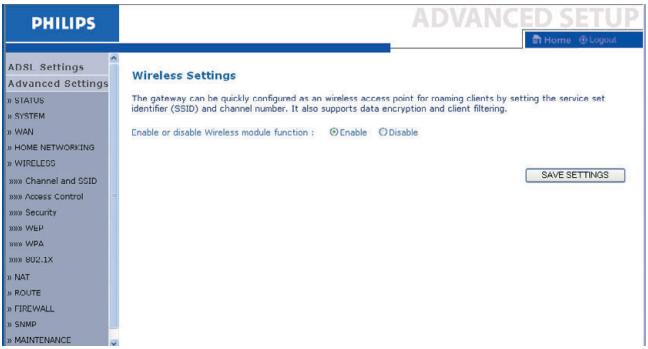


Note: *Remember to configure your client PCs for dynamic address allocation.*
(See page 11 for details.)

Parameter	Description
IP Address	The IP address of the ADSL Wireless Base Station.
IP Subnet Mask	The subnet mask of the network.
DHCP Server	The ADSL Wireless Base Station comes with the DHCP function. Enable this function to dynamically assign an IP address to client PCs.
Lease Time	Set the IP lease time. For home networks this may be set to Forever, which means there is no time limit on the IP address lease.
Start IP Address	Specify the start IP address of the DHCP pool. Do not include the gateway address of the ADSL Wireless Base Station in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e., 192.168.1.xxx.
End IP Address	Specify the end IP address of the DHCP pool.
Domain Name	If your network uses a domain name, enter it here. Otherwise, leave this field blank.

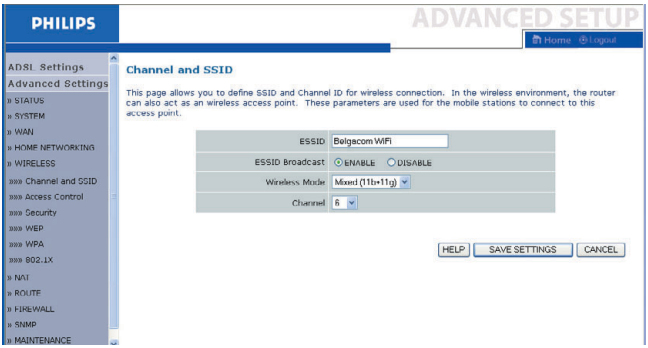
Wireless

The ADSL Wireless Base Station also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, you need to enable the wireless function, define the radio channel, the domain identifier, and the security options.
Check Enable and click 'SAVE SETTINGS'.



Channel and SSID

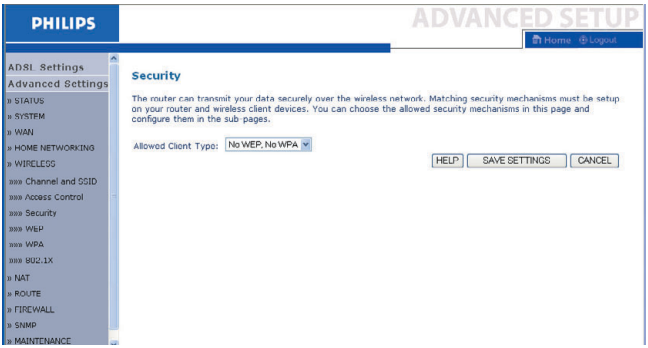
You must specify a common radio channel and SSID (Service Set ID) to be used by the ADSL Wireless Base Station and all of its wireless clients. Make sure you configure all of its clients to the same values.



Parameter	Description
ESSID	Extended Service Set ID. The ESSID must be the same on the ADSL Wireless Base Station and all of its wireless clients.
ESSID Broadcast	Enable or disable the broadcasting of the SSID.
Wireless Mode	This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have.
Channel	The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the ADSL Wireless Base Station and all of its wireless clients. The ADSL Wireless Base Station will automatically assign itself a radio channel, or you may select one manually.

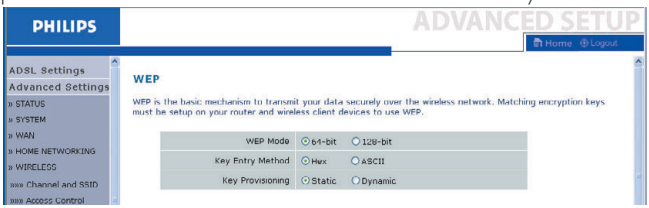
Security

To make your wireless network safe, you should turn on the security function. The ADSL Wireless Base Station supports WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected), and 802.1x security mechanisms.

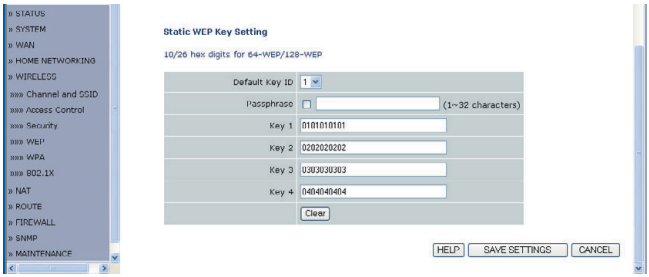


WEP

If you use WEP to protect your wireless network, you need to set the same parameters for the ADSL Wireless Base Station and all your wireless clients.



Parameter	Description
WEP Mode	Select 64 bit or 128 bit key to use for encryption.
Key Entry Method	Select Hex or ASCII code for encryption key generation.
Key Provisioning	Select Static if there is only one fixed key for encryption. If you want to select Dynamic, you would need to enable 802.1x function first.
Key Provisioning	Select Static if there is only one fixed key for encryption. If you want to select Dynamic, you would need to enable 802.1x function first.



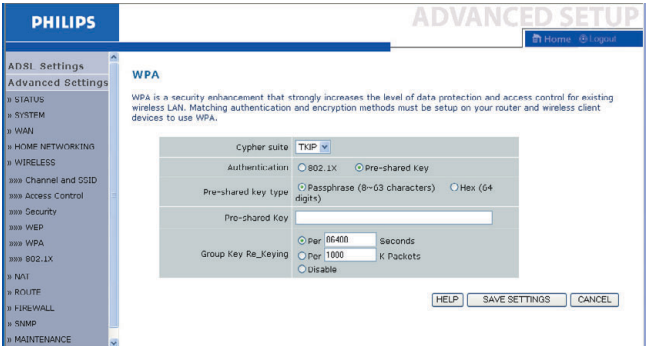
You may automatically generate encryption keys or manually enter the keys. To generate the key automatically with passphrase, check the Passphrase box, enter a string of characters. Select the default key from the drop down menu. Click 'SAVE SETTINGS'.

Note: *The passphrase can consist of up to 32 alphanumeric characters.*

To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F.) Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

WPA

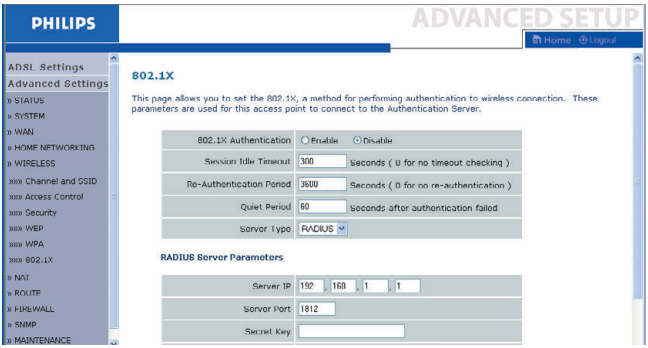
Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1x mechanisms. It provides dynamic key encryption and 802.1x authentication service.



Parameter	Description
Cypher suite	The security mechanism used in WPA for encryption.
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. • 802.1X: for the enterprise network with a RADIUS server. • Pre-shared key: for the SOHO network environment without an authentication server.
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Type in the key here.
Group Key Re-Keying	The period of renewing broadcast/multicast key.

802.1X

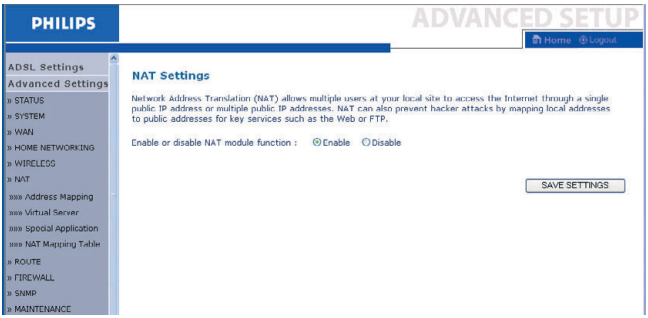
If 802.1x is used in your network, then you should enable this function for the ADSL Wireless Base Station. These parameters are used for the ADSL Wireless Base Station to connect to the authentication server.



Parameter	Description
802.1X Authentication	Enable or disable this authentication function.
Session Idle timeout	Defines a maximum period of time for which the connection is maintained during inactivity.
Re-Authentication Period	Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client.
Quiet Period	Defines a maximum period of time for which the ADSL Wireless Base Station will wait between failed authentications.
Server Type	RADIUS authentication server.
RADIUS Server Parameters	
Server IP	The IP address of your authentication server.
Server Port	The port used for the authentication service.
Secret Key	The secret key shared between the authentication server and its clients.
NAS-ID	Defines the request identifier of the Network Access Server.

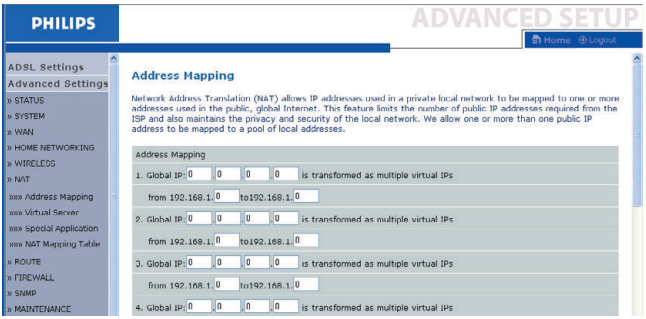
NAT

Network Address Translation allows multiple users to access the Internet sharing one public IP.



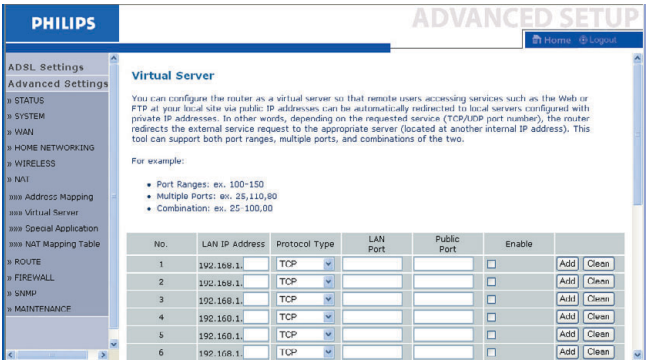
Address Mapping

Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP into the 'from' field.



Virtual Server

If you configure the ADSL Wireless Base Station as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the ADSL Wireless Base Station redirects the external service request to the appropriate server (located at another internal IP address).

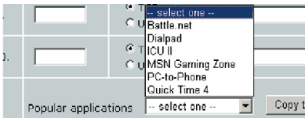


For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.1.2/80, then all HTTP requests from outside users will be transferred to 192.168.1.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

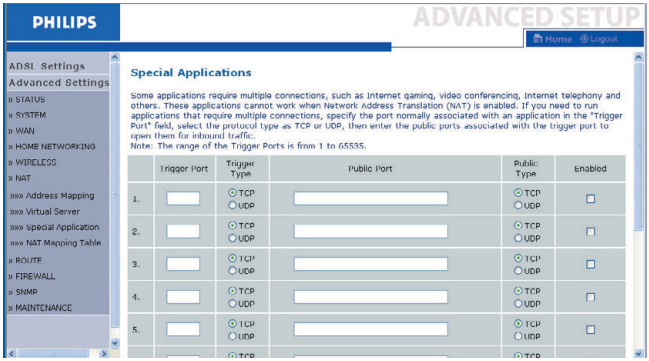
A list of ports is maintained at the following link:
http://www.iana.org/assignments/port-numbers.

Special Applications

Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony.



These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these pages to specify the additional public ports to be opened for each application.



NAT Mapping Table

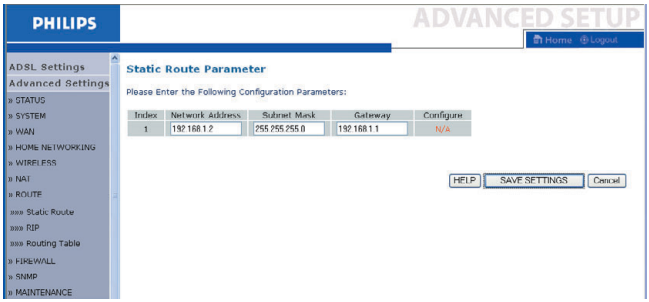
This page displays the current NAPT (Network Address Port Translation) address mappings.

Route

These pages define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.

Static Route

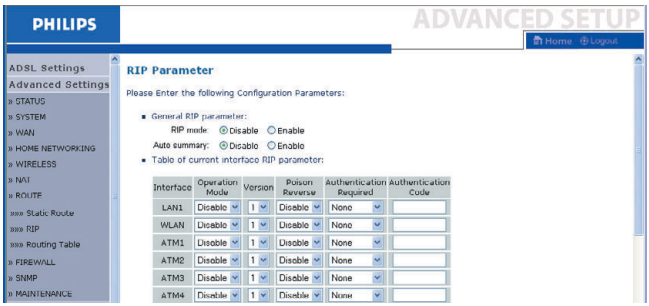
Click 'Add' to add a new static route to the list.



Parameter	Description
Network Address	Enter the IP address of the remote computer for which to set a static route.
Subnet Mask	Enter the subnet mask of the remote network for which to set a static route.
Gateway	Enter the WAN IP address of the gateway to the remote network.

Click 'Save Settings' to save the configuration.

RIP

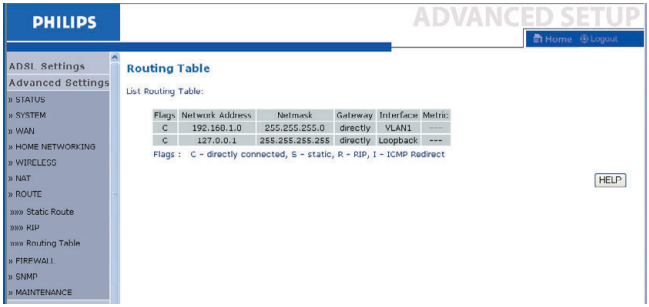


Parameter	Description
General RIP Parameters	
• RIP mode	Globally enables or disables RIP.
• Auto summary	If Auto summary is disabled, then RIP packets will include sub-network information from all subnetworks connected to the router. If enabled, this sub-network information will be summarized to one piece of information covering all subnetworks.
Table of current Interface RIP parameter	
• Interface	The WAN interface to be configured.
• Operation Mode Disable:	RIP disabled on this interface.
• Enable:	RIP enabled on this interface.
• Silent:	Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts.
Version	Sets the RIP (Routing Information Protocol) version to use on this interface.
Poison Reverse	A method for preventing loops that would cause endless retransmission of data traffic.
Authentication Required	• None: No authentication. • Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets.
Authentication Code	Password Authentication key.

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. RIP routers maintain only the best route to a destination.

After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.

Routing Table



Parameter	Description
Flags	Indicates the route status: C = Direct connection on the same subnet. S = Static route. R = RIP (Routing Information Protocol) assigned route. I = ICMP (Internet Control Message Protocol) Redirect route.
Network Address	Destination IP address.
Netmask	The subnetwork associated with the destination. This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a '1' is part of the subnet mask number; each bit that corresponds to '0' is part of the host number.
Gateway	The IP address of the router at the next hop to which frames are forwarded.
Interface	The local interface through which the next hop of this route is reached.
Metric	When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table.

Firewall

The ADSL Wireless Base Station's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks.

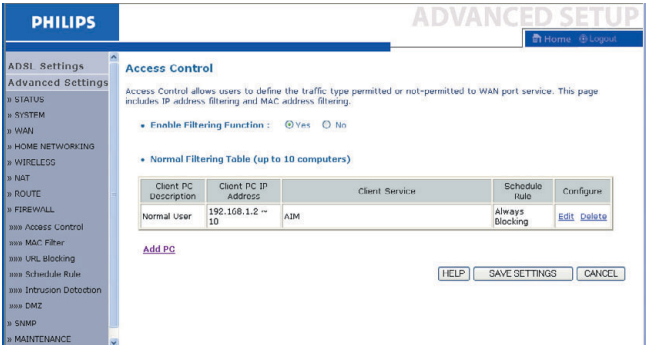
Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The ADSL Wireless Base Station firewall function protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (See page 48-50 for details.)

The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network. Select Enable and click the 'SAVE SETTINGS' button to open the Firewall submenus.

Access Control

Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.



The following items are on the Access Control screen:

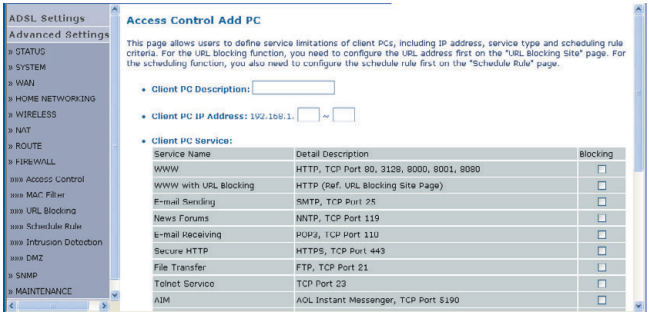
Parameter	Description
Enable Filtering Function	Click Yes to turn on the filtering function.
Normal Filtering Table	Displays the IP address (or an IP address range) filtering table.

To add the PC to the filtering table:

1 Click 'Add PC' on the Access Control screen.

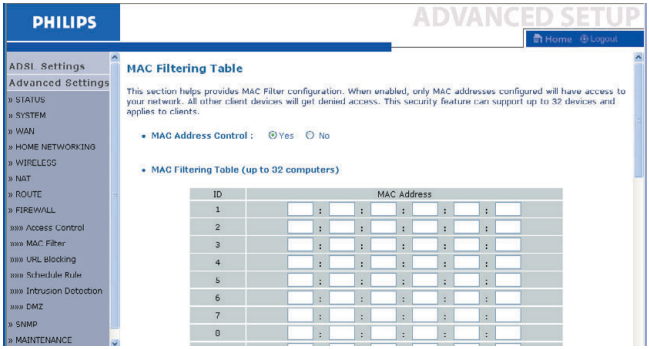
2 Define the appropriate settings for client PC services.

3 Click 'OK' and then click 'SAVE SETTINGS' to save your settings.



MAC Filter

The ADSL Wireless Base Station can also limit the network access based on the MAC address. The MAC Filtering Table allows the ADSL Wireless Base Station to enter up to 32 MAC addresses that are not allowed access to the WAN port.

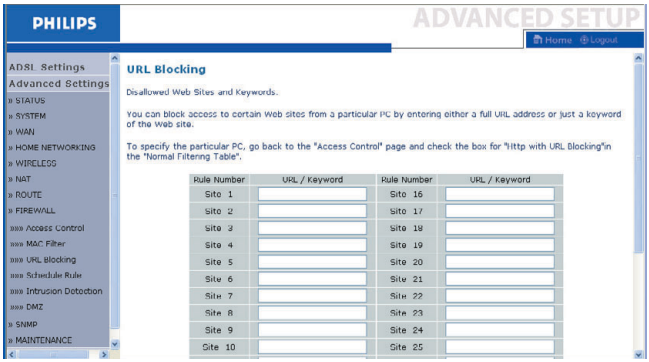


Click Yes to enable, or No to disable this function.

Enter the MAC address in the space provided and click 'Save Settings' to confirm.

URL Blocking

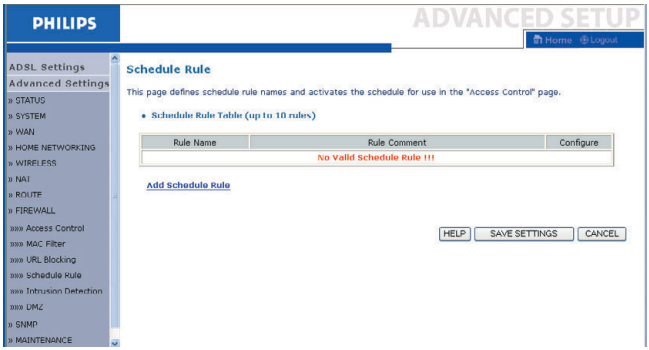
The ADSL Wireless Base Station allows the user to block access to web sites by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.



You can define up to 30 sites here.

Schedule Rule

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the time schedule on this page, and apply the rule on the Access Control page.

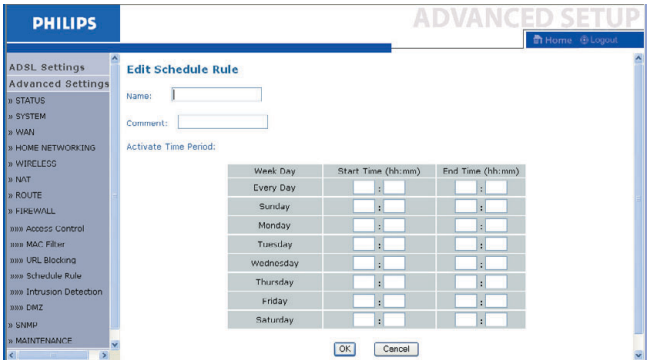


Follow these steps to add a schedule rule:

1 Click 'Add Schedule Rule'.

2 Define the appropriate settings for a schedule rule (as shown in this example).

3 Click 'OK' and then click 'SAVE SETTINGS' to save your settings.



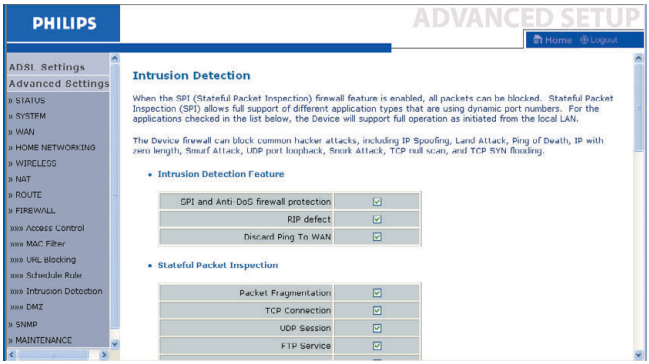
Intrusion Detection

Intrusion Detection Feature

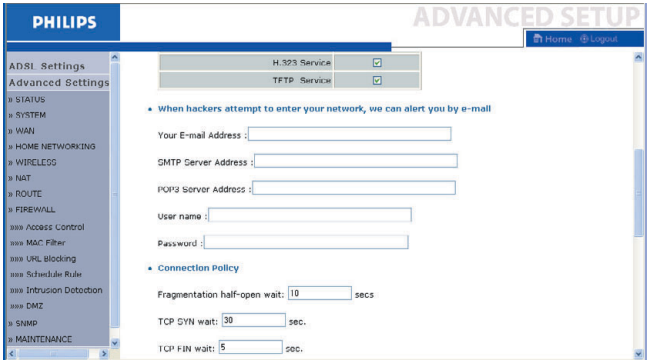
Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: Enabled) - The Intrusion Detection Feature of the ADSL Wireless Base Station limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked in the Stateful Packet Inspection section.

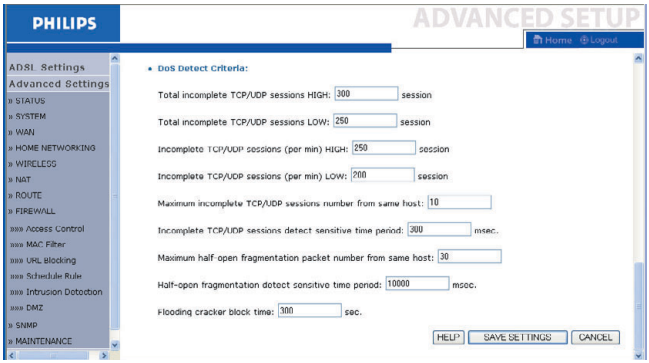
RIP Defect (Default: Disabled) - If an RIP request packet is not acknowledged to by the router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets from accumulating.

Discard Ping to WAN (Default: Disabled) - Prevent a ping on the ADSL Wireless Base Station's WAN port from being routed to the network.



Scroll down to view more information.





Stateful Packet Inspection

This is called a 'stateful' packet inspection because it examines the contents of the packet to determine the state of the communications; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested.

When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks 'FTP Service' in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.

Stateful Packet Inspection allows you to select different application types that are using dynamic port numbers. If you wish to use the Stateful Packet Inspection (SPI) to block packets, click on the Yes radio button in the 'Enable SPI and Anti-DoS firewall protection' field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, or TFTP Service.

- **When hackers attempt to enter your network, we can alert you by e-mail**

If the mail server needs to authenticate your identification before sending out any e-mail, please fill related information in POP3 server, username and password fields. Otherwise leave the three fields blank.

Connection Policy
Enter the appropriate values for TCP/UDP sessions as described in the following table.

Parametre	Defaults	Description
Fragmentation half-open wait	10 sec	Configures the number of seconds that a packet state structure remains active. When timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet.
TCP SYN wait	30 sec	Defines how long the software will wait for a TCP session to synchronize before dropping the session.
TCP FIN wait	5 sec	Specifies how long a TCP session will be maintained after the firewall detects a FIN packet.
TCP connection idle timeout	3600 sec (1 hour)	The length of time for which a TCP session will be managed if there is no activity.
UDP session idle timeout	30 sec	The length of time for which a UDP session will be managed if there is no activity.

DoS Criteria and Port Scan Criteria

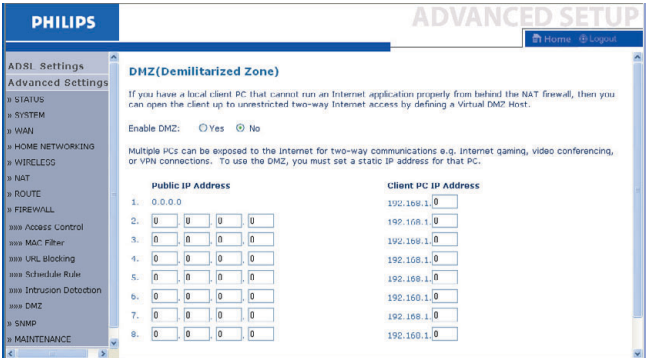
Set up DoS and port scan criteria in the spaces provided (as shown below).

Parametre	Defaults	Description
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of new unestablished sessions that will cause the software to stop deleting halfopen sessions.
Incomplete TCP/UDP sessions (per min) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per minute.
Incomplete TCP/UDP sessions (per min) LOW	200 sessions	Minimum number of allowed incomplete TCP/UDP sessions per minute.
Max. incomplete TCP/ UDP sessions number from same host	10	Maximum number of incomplete TCP/UDP sessions from the same host.
Incomplete TCP/ UDP sessions detect sensitive time period	300 msec	Length of time before an incomplete TCP/UDP session is detected as incomplete.
Maximum half-open fragmentation packet number from same host	30	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	10000 msec	Length of time before a half-open fragmentation session is detected as half-open.
Flooding cracker block time	300 sec	Length of time from detecting a flood attack to blocking the attack.

Note: *The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.*

DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

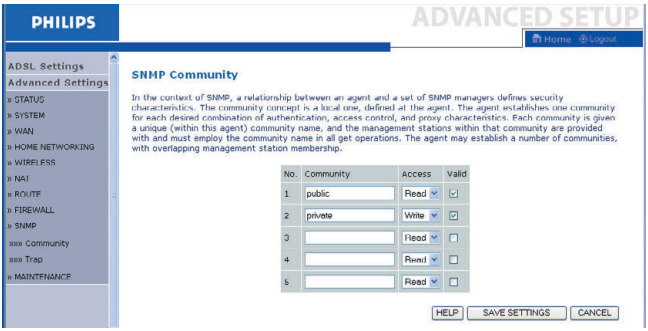


SNMP

Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP).

Community

A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the ADSL Wireless Base Station, the NMS must first submit a valid community string for authentication.

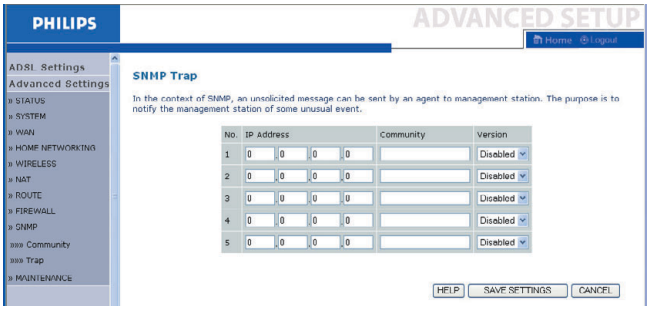


Parameter	Description
Community	A community name authorized for management access.
Access	Management access is restricted to Read Only (Read) or Read/Write (Write).
Valid	Enables/disables the entry.

Note: *Up to five community names may be entered.*

Trap

Specify the IP address of the NMS to notify when a significant event is detected by the agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMS specified as a trap receiver.



Parameter	Description
IP Address	Traps are sent to this address when errors or specific events occur on the network.
Community	A community string (password) specified for trap management. Enter a word, something other than public or private, to prevent unauthorized individuals from accessing information on your system.
Version	Sets the trap status to disabled, or enabled with V1 or V2c. The v2c protocol was proposed in late 1995 and includes enhancements to v1 that are universally accepted. These include a get-bulk command to reduce network management traffic when retrieving a sequence of MIB variables, and a more elaborate set of error codes for improved reporting to a Network Management Station.

Finding the MAC address of a Network Card

Windows 98/ME

Click Start/Run. Type 'winipcfg' and press 'ENTER'.

The MAC address is in the 'Adapter Address' section.

Windows NT4/2000/XP

Click Start/Programs/Command Prompt. Type 'ipconfig /all' and press 'ENTER'.

The MAC address is listed as the 'Physical Address.'

Macintosh

Click System Preferences/Network.

The MAC address is listed as the 'Ethernet Address' on the TCP/IP tab.

Linux

Run the command '/sbin/ifconfig.'

Maintenance

Use the Maintenance menu to backup the current configuration, restore a previously saved configuration, restore factory settings, update firmware, and reset the ADSL Wireless Base Station.

Configuration Tools

Choose a function and click Next.

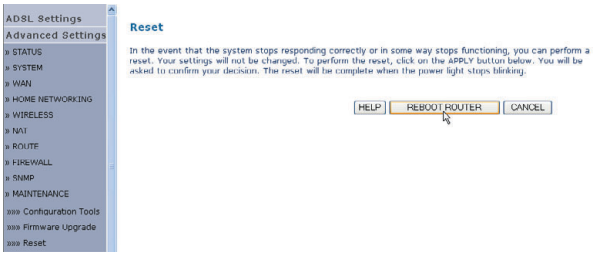
Backup allows you to save the ADSL Wireless Base Station's configuration to a file. Restore can be used to restore the saved backup configuration file. Restore to Factory Defaults resets the ADSL Wireless Base Station to the original settings. You will be asked to confirm your decision.

Firmware Upgrade

Use the Firmware Upgrade screen to update the firmware or user interface to the latest versions. Download the upgrade file, and save it to your hard drive. Then click 'Browse...' to look for the downloaded file. Click 'BEGIN UPGRADE'. Check the Status page Information section to confirm that the upgrade process was successful.

Reset

Click 'REBOOT ROUTER' to reset the ADSL Wireless Base Station.

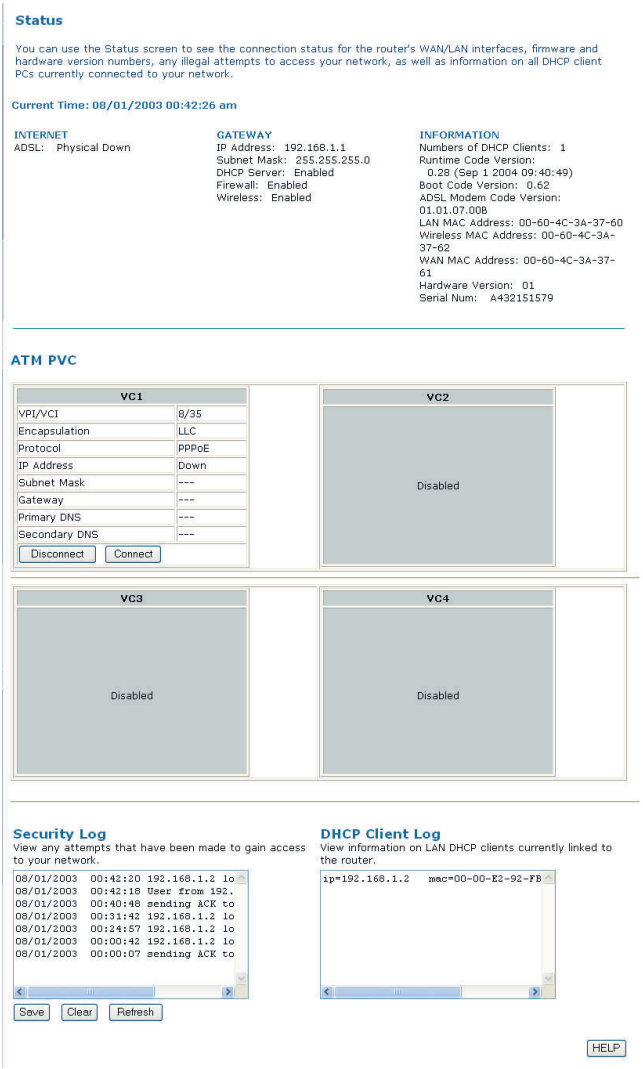


If you perform a reset from this page, the configurations will not be changed back to the factory default settings.

Note: *If you use the Reset button on the rear panel, the ADSL Wireless Base Station performs a power reset. Press the button for over five seconds, and the factory default settings will be restored.*

Status

The Status page displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network. The security log may be saved to a file by clicking 'Save' and choosing a location.



The following items are included on the Status page:

Item	Description
INTERNET	Displays WAN connection type and status. Click the Connect button to connect to your ISP.
GATEWAY	Displays system IP settings, as well as DHCP Server and Firewall status.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and for the ADSL Wireless Base Station, as well as the hardware version and serial number.
Security Log • Save • Clear • Refresh	Displays illegal attempts to access your network. Click on this button to save the security log file. Click on this button to delete the access log. Click on this button to refresh the screen.
DHCP Client Log	Displays information on DHCP clients on your network.

How to set-up a computer network?

The next pages will show you an example of how to set-up a computer network using the Philips ADSL Wireless Base Station.

Warning:

The ADSL Wireless Base Station only establishes a connection between your wireless network devices. How you use this connection is up to you.

Setting-up a computer network is to be seen as an independent application that requires networking software from other manufacturers.
For example, the networking software that has been incorporated in the Windows Operating System by Microsoft.

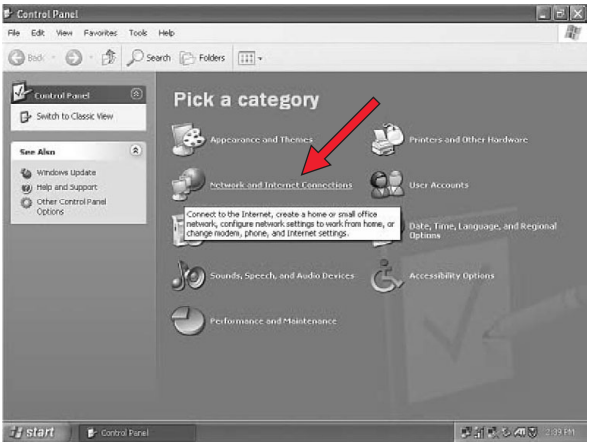
Therefore, the description below is to be seen as an example only.

WHAT IS YOUR WINDOWS VERSION?

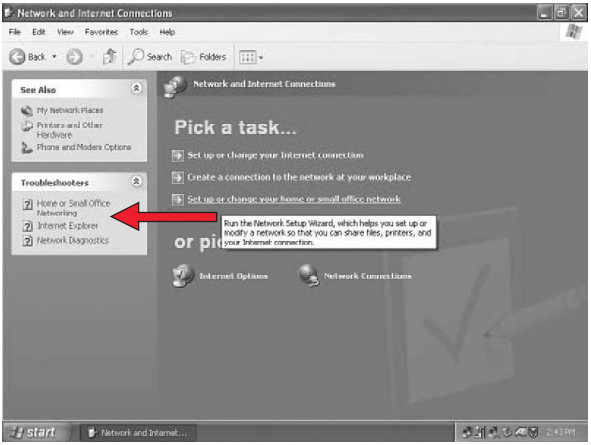
1. Start setting-up your network with the computer that has the latest operating system. The order of preference being: Windows XP, Windows 2000, Windows Me, and finally Windows 98SE.
2. Use its Networking Setup Wizard and allow it to make a networking setup diskette.
3. With this diskette, set-up your remaining computers.

For Windows XP and Windows 2000.
See further on in this chapter for Windows Me and Windows 98SE.

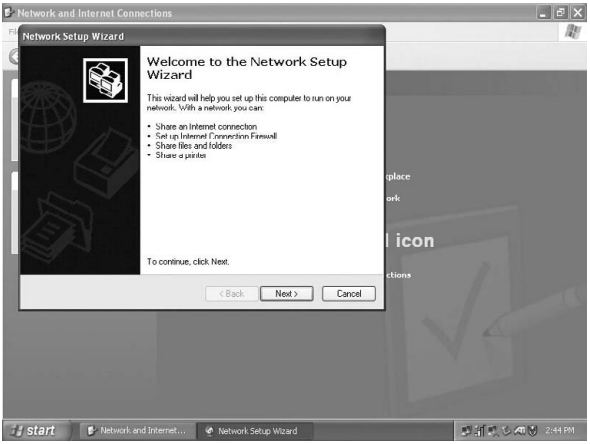
Click the Windows Start button, and click "Control Panel" from the list.



Double-click the "Network and Internet connections" icon.



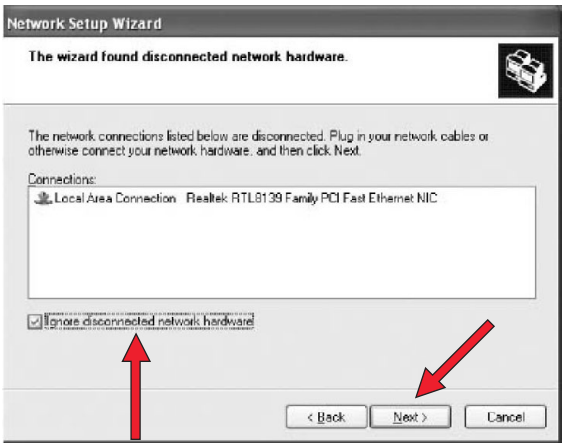
Click in the list to the left on "Setting-up a home network or small business network".



The Wizard Network Setup appears. Click 'Next' to continue.

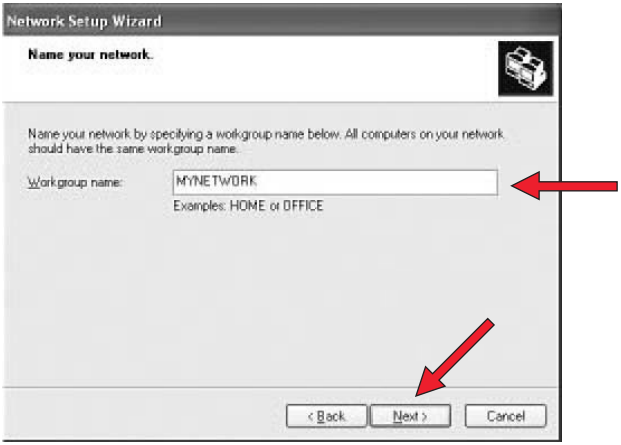
Wizard Network Settings

1. Please, carefully read the instructions the Wizard gives you, and adapt your choices to the type of network you want to set-up. Use the Help feature within the Wizard if you need more information while using the Wizard.
2. In each window, click 'Next' to go to the next step.
3. Below, we will describe some of the crucial steps of this Wizard.



Place a check mark to ignore any broken network connections before clicking 'Next' to continue.

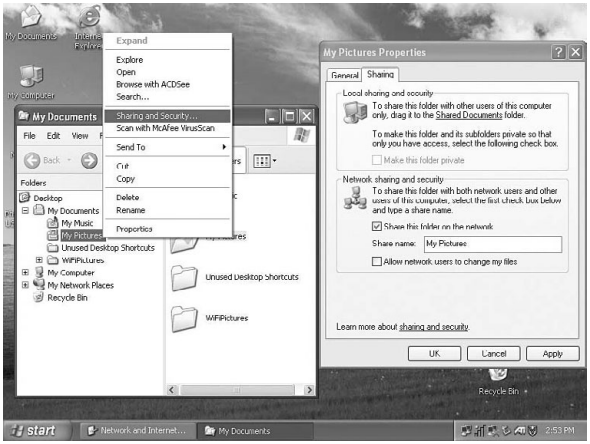
1. Enter a description that helps you recognize the computer.
2. Enter a name that is different for each computer.
3. Click 'Next' to continue.



Enter the same workgroup name for all computers in the network, then click 'Next' to continue.

Choose to make a networking setup disk. Then click 'Next'.

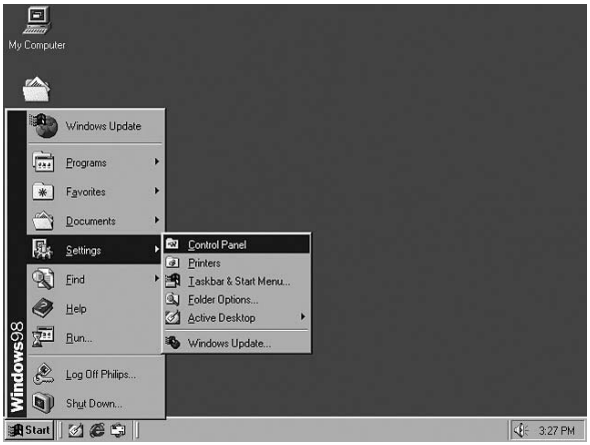
Click 'Finish' to close the Wizard, and then use the disk you made to set-up your other computers.



To share folders with the network: Start Windows Explorer and right-click the folder you wish to share with the network. Click the 'Sharing' tab and adapt the settings.

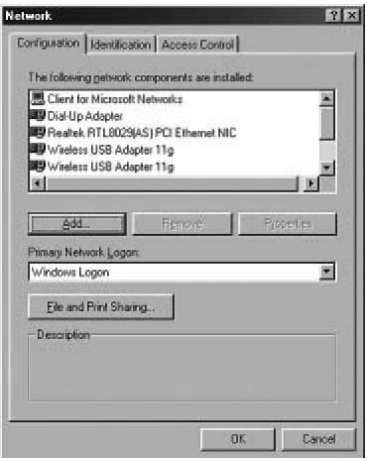
To explore the network: Double-click the Network Environment icon on the desktop.
If you need more information, consult Windows Help.

For Windows 98SE and Windows Me.
See earlier on in this chapter for Windows XP and Windows 2000.

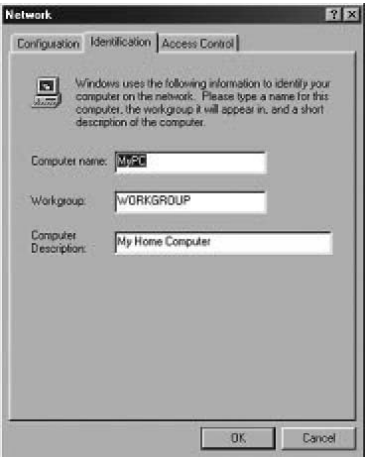


Click the Windows Start button, click "Settings", and click "Control Panel" from the list.

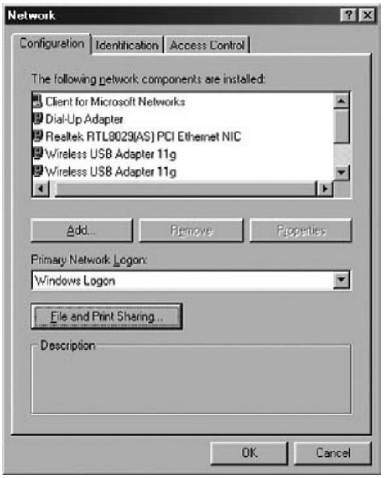
Double-click the "Network" icon.



Click the 'Identification' tab.

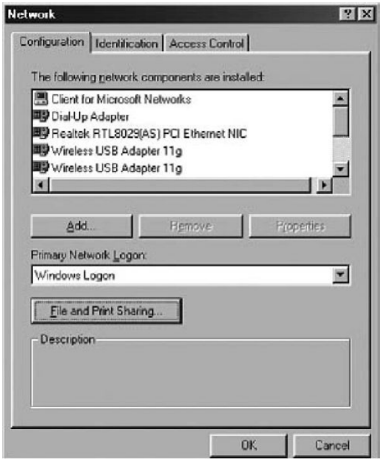


1. Enter a name that is different for each computer.
2. Enter the same workgroup name for all computers in the network.
3. Enter a description that helps you recognize the computer.
4. Click on the 'Configuration' tab to continue.

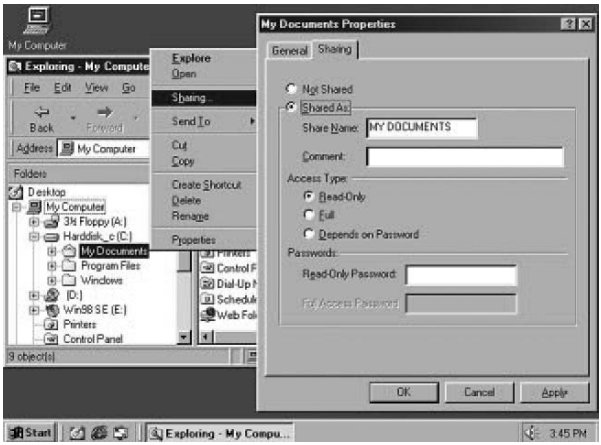


Click the 'Sharing files and printers' button.

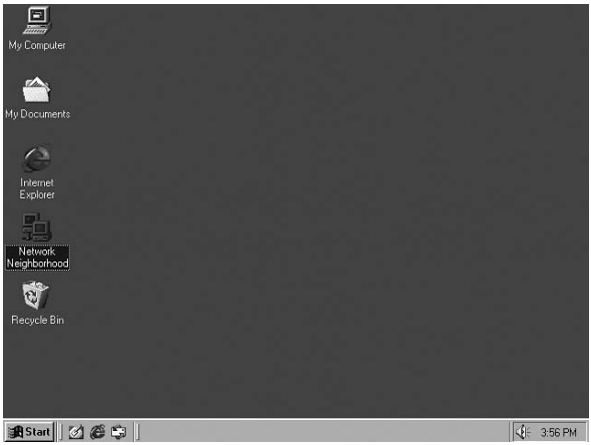
Select the access options you want, and click 'OK' to continue.



Click 'OK' to accept the changes.



To share folders with the network: Start Windows Explorer and right-click the folder you wish to share with the network. Click the 'Sharing' tab and adapt the settings.



To explore the network: Double-click the Network Environment icon on the desktop.
If you need more information, consult Windows Help.

Troubleshooting

This section describes common problems you may encounter and possible solutions to them. The ADSL Wireless Base Station can be easily monitored through panel indicators to identify problems.

Problem	Solution
Power LED is Off	• Check connections between the ADSL Wireless Base Station, the external power supply, and the wall outlet. • If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.
Link LED is Off	• Verify that the ADSL Wireless Base Station and attached device are powered on. • Be sure the cable is plugged into both the ADSL Wireless Base Station and the corresponding device. • Verify that the proper cable type is used and that its length does not exceed the specified limits. • Make sure that the network interface on the attached device is configured for the proper communication speed and duplex mode. • Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.
Cannot ping the ADSL Wireless Base Station from the attached LAN	• Verify that the IP addresses are properly configured. For most applications, you should use the ADSL Wireless Base Station's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the ADSL Wireless Base Station and any attached LAN devices. • Make sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP.
Cannot connect using the web browser	• Be sure to have configured the ADSL Wireless Base Station with a valid IP address, subnet mask, and default gateway. • Check that you have a valid network connection to the ADSL Wireless Base Station and that the port you are using has not been disabled. • Check the network cabling between the management station and the ADSL Wireless Base Station.
Forgot or lost the password	• Press the Reset button on the rear panel (holding it down for at least five seconds) to restore the factory defaults.

Problem	Solution
Power LED is Off	• Check connections between the ADSL Wireless Base Station, the external power supply, and the wall outlet. • If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.
A wireless PC cannot associate with the ADSL Router	• Make sure the wireless PC has the same SSID settings as the ADSL Wireless Base Station. See 'Channel and SSID' on page 36. • You need to have the same security settings on the clients and the ADSL Wireless Base Station. See 'Security' on page 36.
The wireless network is often interrupted	• Move your wireless PC closer to the ADSL Wireless Base Station to find a better signal. If the signal is still weak, change the angle of the antenna. • There may be interference, possibly caused by a microwave ovens or wireless phones. Change the location of the interference sources or of the ADSL Wireless Base Station. • Change the wireless channel on the ADSL Wireless Base Station. See 'Channel and SSID' on page 36. • Check that the antenna, connectors, and cabling are firmly connected.
The ADSL Wireless Base Station cannot be detected by a wireless client	• The distance between the ADSL Wireless Base Station and wireless PC is too great. • Make sure the wireless PC has the same SSID and security settings as the ADSL Wireless Base Station. See ADSL Wireless Base Station. See 'Channel and SSID' on page 36 and 'Security' on page 36.

Specifications

Physical Characteristics

Ports
– Four 10/100Mbps RJ-45 Ports
– One ADSL RJ-11

ADSL Features
– Supports DMT line modulation
– Supports Annex A Full-Rate ADSL: up to 8 Mbps downstream, up to 1 Mbps upstream (G.992.1 &T1.413, Issue 2)
– Supports G.Lite ADSL: up to 1.5 Mbps downstream, up to 512 Kbps upstream
– Dying GASP support

ATM Features
– RFC1483 Encapsulation (IP, Bridging and encapsulated routing)
– PPP over ATM (LLC &VC multiplexing) (RFC2364)
– Classical IP (RFC1577)
– Traffic shaping (UBR, CBR)
– OAM F4/F5 support
– PPP over Ethernet Client

Management Features
– Firmware upgrade via web based management
– Web based management (configuration)
– Power indicators
– Event and history logging
– Network ping

Security Features
– Password protected configuration access
– User authentication (PAP/CHAP) with PPP
– Firewall NAT NAPT
– VPN pass through (IPSec-ESP Tunnel mode,L2TP, PPTP)

LAN Features
– IEEE 802.1d (self-learning transparent Bridging)
– DHCP Server
– DNS Proxy
– Static Routing, RIPv1 and RIP

Radio Features
– Wireless RF module Frequency Band
– 802.11g Radio: 2.4GHz
– 802.11b Radio: 2.4GHz
Europe - ETSI
– 2412~2472MHz (Ch1~Ch13)

Modulation Type
– OFDM, CCK

Operating Channels IEEE 802.11b compliant:
– 13 channels (ETSI)

Operating Channels IEEE 802.11g compliant:
– 13 channels (Europe)

RF Output Power Modulation Rate-Output Power (dBm)
802.11b - 1Mbps (16 dBm)
802.11b - 2Mbps (16 dBm)
802.11b - 5.5Mbps (16 dBm)
802.11b - 11Mbps (16 dBm)

Modulation Rate-Output Power (dBm)
802.11g - 6Mbps (15 dBm)
802.11g - 9Mbps (15 dBm)
802.11g - 12Mbps (15 dBm)
802.11g - 18Mbps (15 dBm)
802.11g- 24Mbps (15 dBm)
802.11g - 36Mbps (15 dBm)
802.11g- 48Mbps (15 dBm)
802.11g - 54Mbps (15 dBm)

Sensitivity Modulation Rate-
Receiver 2.412 ~ 2.484 HGz Sensitivity (dBm)
802.11b - 1Mbps - (90 dBm)
802.11b - 2Mbps - (88 dBm)
802.11b - 5.5Mbps - (85 dBm)
802.11b- 11Mbps - (84 dBm)

Modulation Rate-Receiver Sensitivity Typical (dBm)
802.11g - 6Mbps - (88 dBm)
802.11g - 9Mbps - (87 dBm)
802.11g - 12Mbps - (84 dBm)
802.11g - 18Mbps - (82 dBm)
802.11g - 24Mbps - (79 dBm)
802.11g - 36Mbps - (75 dBm)
802.11g - 48Mbps - (68 dBm)
802.11g - 54Mbps - (68 dBm)

Environmental

Complies with the following standards:

Temperature: IEC 68-2-14
0 to 50 degrees C (Standard Operating)
-40 to 70 degree C (Non-operation)

Humidity
10% to 90% (Non-condensing)

Vibration
IEC 68-2-36, IEC 68-2-6

Shock
IEC 68-2-29

Drop
IEC 68-2-32

Input Power
12 V 1 A

IEEE Standards
IEEE 802.3, 802.3u, 802.11g, 802.1d
ITU G.dmt
ITU G.Handshake
ITU T.413 issue 2 - ADSL full rate

Standards Conformance Electromagnetic Compatibility
CE, ETSI, R&TTE, ETS 300 328, ETS 300 826

Safety
EN60950

Internet Standards
RFC 826 ARP
RFC 791 IP
RFC 792 ICMP
RFC 768 UDP
RFC 793 TCP
RFC 783 TFTP
RFC 1483 AAL5 Encapsulation
RFC 1661 PPP
RFC 1866 HTML
RFC 2068 HTTP
RFC 2364 PPP over ATM

Hereby, Philips Consumer Electronics, BLC P&A CC, declares that this CPWBS154 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Hierbij verklaart, Philips Consumer Electronics, BLC P&A CC dat het toestel CPWBS154 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Par la présente, Philips Consumer Electronics, BLC P&A CC, déclare que l'appareil CPWBS154 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Hiermit erklärt Philips Consumer Electronics, BLC P&A CC die Übereinstimmung des Gerätes CPWBS154 mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG.

CPWBS154

B ✔	DK ✘	E ✘	GR ✘	F ✘
IRL ✘	I ✘	L ✘	NL ✘	A ✘
P ✘	SU ✘	S ✘	UK ✘	N ✘
D ✘	CH ✘			

October 2004

PHILIPS

AQ95-56F-568KR
(report No.)

EC DECLARATION OF CONFORMITY

We , Philips Consumer Electronics, P&A CC: Building SBP6
(manufacturer's name)

P.O.Box 80002, 5600 JB Eindhoven, The Netherlands
(manufacturer's address)

declare under our responsibility that the electrical product:

Philips
(name)

CPWBS154/18
(type or model)

ADSL Wireless Base Station
(product description)

to which this declaration relates is in conformity with the following standards:

EN 300 328 v1.4.1 (04-2003)
EN 301 489-1 v1.3.1 (09-2001)
EN 301 489-17 v1.2.1 (08-2002)
EN61000-3-2:2000
EN61000-3-3:1995 +A1:2001
EN55022:1998 + A1:2000 + A2:2003
EN55024:1998 + A1:2001 + A2:2003
IEC 60950-1 :2001

(title and/or number and date of issue of the standards)

following the provisions of 1999/5/EC (R&TTE Directive)
and is produced by a manufacturing organisation on ISO 9000 level.

Eindhoven, 01/10/2004
(place, date)

K.Rysman
Approbation manager
(signature, name and function)

www.philips.com
This document is printed on chlorine free produced paper
Data subject to change without notice

CE 0682 ⓘ

PHILIPS